Ανοικτό Πανεπιστήμιο Κύπρου
Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή

Στην Ασφάλεια Υπολογιστών και Δικτύων

Εφαρμογή Του Πρότυπου ISO 27001 Για Την Ασφάλεια Των Mobile Agents

Γεώργιος Χατζηκυριάκου

Επιβλέπουσα Καθηγήτρια
Δρ. Αδαμαντίνη Περατικού

Μάϊος 2019

Ανοικτό Πανεπιστήμιο Κύπρου
Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Εφαρμογή Του Πρότυπου ISO 27001 Για Την Ασφάλεια Των Mobile Agents

Γεώργιος Χατζηκυριάκου

Επιβλέπουσα Καθηγήτρια
Δρ. Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση
μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάϊος 2019

Περίληψη

Οι mobile agents είναι μια μορφή mobile code που έχουν την δυνατότητα να κινούνται αυτόνομα σε μια προκαθορισμένη ή δυναμική διαδρομή από host σε host και να εκτελούν προκαθορισμένο κώδικα, χρησιμοποιώντας πόρους του εκάστοτε host. Το γεγονός ότι έχουν την δυνατότητα να κινούνται αυτόνομα μεταφέροντας τον κώδικα προς εκτέλεση, δεδομένα αλλά και την κατάσταση της εκτέλεσης τους, τους καθιστά ευάλωτους σε διάφορους τύπους επιθέσεων.

Ο σκοπός αυτής της διατριβής είναι να εξεταστεί κατά πόσο οι απαιτήσεις του διεθνούς πρότυπου ISO 27001 μπορεί να χρησιμοποιηθούν για την ασφάλεια των mobile agents. Για τον σκοπό αυτό, δημιουργήσαμε έναν οργανισμό-μοντέλο και τοποθετήσαμε μέσα σε αυτό το πλαίσιο, μεταξύ άλλων περιουσιακών στοιχείων και τους mobile agents. Στην συνέχεια υλοποιήσαμε τις απαιτήσεις του προτύπου παράγραφο προς παράγραφο για να δημιουργήσουμε στο τέλος ένα σύστημα διαχείρισης ασφάλειας πληροφοριών (ΣΔΑΠ).

Μέσα από την διαδικασία της διαχείρισης κινδύνων και με την βοήθεια μελετών άλλων ερευνητών, μπορέσαμε να προσδιορίσουμε τους κινδύνους που μπορούν να απειλήσουν τους mobile agents και να εφαρμόσουμε τους κατάλληλους ελέγχους, για τον μετριασμό των επιπτώσεων. Μέσω αυτών των ελέγχων, δημιουργήσαμε πολιτικές και διαδικασίες ασφαλείας για να διασφαλίσουμε την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των περιουσιακών στοιχείων του οργανισμού και κατά συνέπεια των mobile agents.

Τέλος, δημιουργήσαμε τέσσερα ρεαλιστικά σενάρια σχετικά με την ασφάλεια των mobile agents και μελετήσαμε ορισμένες περιπτώσεις ώστε να δοκιμάσουμε την αποτελεσματικότητα του ΣΔΑΠ και να απαντήσουμε στα ερευνητικά ερωτήματα που θέσαμε. Διαπιστώσαμε ότι όλες οι απαιτήσεις του προτύπου συμβάλλουν άμεσα ή έμμεσα στην ασφάλεια των mobile agents. Απαιτήσεις όπως για παράδειγμα: α) η διαχείριση κινδύνων, β) ο καθορισμός και η τήρηση πολιτικών ασφαλείας, γ) η ευαισθητοποίηση του προσωπικού, δ) η διαδικασία εσωτερικού ελέγχου του ΣΔΑΠ αλλά και ε) η συνεχής βελτίωση του ΣΔΑΠ, μπορούν να προσθέσουν όπως θα δούμε, ένα επιπλέον επίπεδο προστασίας στους mobile agents και τις πλατφόρμες τους.

Λέξεις – Κλειδιά: mobile agents, ISO 27001, ασφάλεια πληροφοριών, σύστημα διαχείρισης ασφάλειας πληροφοριών, ΣΔΑΠ, διαχείριση κινδύνων, πολιτικές ασφάλειας, aglets, java, δοκιμή παρείσφρησης

Summary

Mobile Agents is a form of mobile code technology that they have the ability to move autonomously from host to host in a predefined or dynamic route. They can execute a predefined code and handle resources in each host. The fact that mobile agents have the ability to move autonomously carrying the execution code, data, and the execution state, they make them vulnerable in various kinds of attacks.

The purpose of this thesis is to study whether the requirements of the international standard ISO 27001 can be used to make the mobile agents more secure. For this reason, we have created a model organization with mobile agents among other assets. Then, we implemented all requirements of the standard clause by clause, creating that way an Information Security Management System (ISMS).

During the procedure of Risk Management and the guidance of the studies from other researchers, we were able to define the threats that can make the mobile agents vulnerable. Then, we applied security controls to reduce the impact of these threats on the organization. We used these controls, to create security policies and procedures to ensure the confidentiality, integrity, and availability of the assets of the organization and consequently, the security of mobile agents and their platforms.

Finally, we implemented four realistic scenarios to study specific cases related to mobile agent security, in order to test the efficiency of the ISMS and answer the research questions we defined.

We concluded, that all requirements of the standard can contribute directly or indirectly in mobile agent security. Requirements like a) Risk Management, b) Security Policies, c) Awareness, d) Internal Audit and e) Continual Improvement, can contribute in mobile agent security.

Keywords: mobile agents, ISO 27001, information security, information security management system, ISMS, risk management, security policies, aglets, java, penetration testing

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια μου κυρία Αδαμαντίνη Περατικού για την εμπιστοσύνη που μου έδειξε, όπως επίσης για την βοήθεια και την υποστήριξη που μου πρόσφερε κατά την διάρκεια της παρούσας διατριβής.

Επίσης, ευχαριστώ θερμά τους γονείς μου για την συμπαράσταση και υποστήριξη τους καθ' όλη την διάρκεια των μεταπτυχιακών μου σπουδών.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Οι mobile agents είναι μια μορφή mobile code που έχουν την δυνατότητα να κινούνται αυτόνομα σε μια διαδρομή από host σε host και να εκτελούν προκαθορισμένο κώδικα, χρησιμοποιώντας πόρους του εκάστοτε host (Επεξεργαστική ισχύ, μνήμη, αποθηκευτικό χώρο, κ.α.). Σκοπός τους είναι η επιστροφή των αποτελεσμάτων της εκτέλεσης του κώδικα στον host από όπου ξεκίνησαν. Οι mobile agents έχουν πολλές εφαρμογές, όπως: η ανάκτηση πληροφοριών, κατανεμημένα πολυμέσα, πλατφόρμες τηλεδιάσκεψης, ηλεκτρονικό εμπόριο, κ.α. Υπάρχουν δυο τύπων mobile agents. Αυτοί που κινούνται σε μία προκαθορισμένη διαδρομή και αυτοί που κινούνται σε μια δυναμική διαδρομή αυτόνομα και ανάλογα με την κατάσταση του δικτύου.
Πρόκειται για μια τεχνολογία κατανεμημένων συστημάτων που προσφέρει αρκετά πλεονεκτήματα, όπως: μείωση της κίνησης του δικτύου, μείωση εύρους ζώνης του δικτύου (bandwidth), βελτίωση ισχύος και ανοχής του δικτύου, κ.α.
Παρόλα τα θετικά όμως, η ασφάλεια των mobile agents είναι ένα πρόβλημα που απασχόλησε τα τελευταία χρόνια πολλούς ερευνητές και οργανισμούς. Το γεγονός ότι έχουν την δυνατότητα να κινηθούν αυτόνομα από τον ένα host στον άλλο μεταφέροντας κώδικα προς εκτέλεση, δεδομένα αλλά και την κατάσταση της εκτέλεσης τους, τους καθιστά όπως θα δούμε στο Κεφάλαιο 2, ευάλωτους σε διάφορους τύπους επιθέσεων.

1.1 Σκοπός της διατριβής

Ο σκοπός της διατριβής είναι να εξεταστεί κατά πόσο οι απαιτήσεις του διεθνούς πρότυπου ISO 27001 μπορεί να χρησιμοποιηθούν για την ασφάλεια των mobile agents. Τα προσδοκόμενα αποτελέσματα της διατριβής είναι να αποδείξουμε ότι με τις κατάλληλες πολιτικές ασφαλείας και διαδικασίες, το ISO 27001 μπορεί να παρέχει ένα επιπλέον επίπεδο προστασίας.

1.2 Αναγκαιότητα

Το γεγονός ότι οι δημοφιλής πλατφόρμες mobile agent προσφέρουν δυνατότητες όπως: περιβάλλοντα πολλαπλών χρηστών, έλεγχο προσπέλασης, χρήση αλγορίθμων κρυπτογράφησης, διαχείριση πόρων του συστήματος, κ.α., καθιστά τις απαιτήσεις του διεθνούς πρότυπου ISO 27001 κατάλληλο εργαλείο, που θα μπορούσε να συνεισφέρει παρέχοντας ένα επιπλέον επίπεδο προστασίας.

Μελετώντας την διεθνή βιβλιογραφία διαπιστώσαμε ότι δεν υπάρχουν αναφορές για εφαρμογή του ISO 27001 σε περιβάλλον mobile agent.

1.3 Βασικά ερευνητικά ερωτήματα

Τα βασικά ερευνητικά ερωτήματα που θέσαμε είναι:

- Ποιες είναι οι ανάγκες για ασφάλεια στους mobile agents;
- Οι απαιτήσεις του πρότυπου ISO 27001 θα μπορούσαν να παρέχουν ένα επιπλέον επίπεδο προστασίας στα δεδομένα που μεταφέρονται μέσω των mobile agents;
- Η δημιουργία και η εφαρμογή κατάλληλων πολιτικών ασφαλείας και διαδικασιών από τους προγραμματιστές και διαχειριστές συστημάτων, θα μπορούσαν να αποτρέψουν την εκτέλεση κακόβουλου λογισμικού ή/και τη διαρροή ευαίσθητων πληροφοριών από τους mobile agents σε μη εξουσιοδοτημένα άτομα;

1.4 Περιγραφή μεθοδολογίας

Για να απαντηθούν τα ερευνητικά ερωτήματα που θέσαμε ακολουθήσαμε την παρακάτω μεθοδολογία:

Βήμα 1: Ανασκόπηση βιβλιογραφίας και μελέτη των κενών ασφάλειας στους mobile agents μέσω των μελετών που έγιναν από άλλους ερευνητές.

Βήμα 2: Η τοποθέτηση των mobile agents στο πλαίσιο ενός οργανισμού-μοντέλου για την δημιουργία ενός ΣΔΑΠ με βάση τις απαιτήσεις του διεθνούς προτύπου ISO 27001.

Βήμα 3: Θα προσπαθήσουμε να απαντήσουμε τα ερευνητικά ερωτήματα που θέσαμε στην προηγούμενη παράγραφο, μελετώντας κάποια ρεαλιστικά σενάρια περιπτώσεων από τις

απαιτήσεις του ΣΔΑΠ του οργανισμού-μοντέλου που υλοποιήσαμε στο Βήμα 2. Για την μελέτη περιπτώσεων που απαιτούν πρακτική εφαρμογή (προγραμματισμό), δημιουργήσαμε σχετική διαδικασία με τον κύκλο ζωής του λογισμικού.

1.5 Παρουσίαση ενοτήτων

Η διατριβή χωρίζεται σε 5 κεφάλαια:

Στο **Κεφάλαιο 1** γίνεται μια σύντομη εισαγωγή στους mobile agents, δηλώνεται ο σκοπός και η αναγκαιότητα της διατριβής, καθορίζονται τα ερευνητικά ερωτήματα και ορίζεται η μεθοδολογία που θα ακολουθηθεί.

Στο **Κεφάλαιο 2** γίνεται η βιβλιογραφική ανασκόπηση. Σε αυτή την ενότητα γίνετε η μελέτη των πτυχών των mobile agents που αφορούν την εξέλιξη και την ασφάλειά τους. Συγκεκριμένα γίνετε αναφορά:

1. Στην εξέλιξη των mobile agents.
2. Στην ασφάλεια των mobile agents και τους τύπους επιθέσεων.
3. Σύγκριση διάσημων πλατφορμών ως προς την ασφάλεια τους.
4. Σε άλλες προσεγγίσεις για ενίσχυση της ασφάλειας των mobile agents.

Επίσης γίνεται αναφορά:

1. Στο διεθνές πρότυπο ISO 27001.
2. Στην εξέλιξη των προτύπων της οικογένειας ISO 27000.
3. Στην υλοποίηση του ISO 27001.

Στο **Κεφάλαιο 3** ασχοληθήκαμε με την υλοποίηση του συστήματος διαχείρισης πληροφοριών για έναν οργανισμό-μοντέλο που ασχολείται με την ανάπτυξη εφαρμογών και την παροχή υπηρεσιών σε περιβάλλον mobile agents.

Στο **Κεφάλαιο 4** ασχοληθήκαμε με την μελέτη ορισμένων περιπτώσεων, ώστε να δείξουμε τον τρόπο που το διεθνές πρότυπο ISO 27001 μπορεί να προσθέσει ένα επιπλέον επίπεδο ασφαλείας

στους mobile agents και με αυτό τον τρόπο να απαντήσουμε τα ερευνητικά ερωτήματα που θέσαμε.

Στο **Κεφάλαιο 5** απαντάμε στα ερευνητικά ερωτήματα που θέσαμε και κάνουμε αναφορά στους περιορισμούς, αλλά και σε ορισμένα θέματα που θα μπορούσαν να υλοποιηθούν στο μέλλον για την ενίσχυση του οργανισμού-μοντέλου.

Κεφάλαιο 2
Βιβλιογραφική Ανασκόπηση

2.1 Η εξέλιξη των mobile agents

Η ιδέα της αποστολής και της εκτέλεσης απομακρυσμένου κώδικα χρονολογείτε από την αρχή της δημιουργίας του διαδικτύου, δηλαδή στα τέλη της δεκαετίας του 60'. Συγκεκριμένα, ή γλώσσα προγραμματισμού DEL (Decode-Encode Language) μπορούσε να τρέξει διαδραστικά προγράμματα σε απομακρυσμένες κονσόλες, μέσω δικτύου. Αργότερα, η προσέγγιση αυτή εμφανίστηκε και από άλλα ανεξάρτητα έργα, όπως το Softnet και το Network Command Language.

Στις αρχές της δεκαετίας του 80' παρουσιάστηκε από τους Birrell και Nelson το διάσημο αρχιτεκτονικό μοντέλο κατανεμημένων συστημάτων πελάτη/εξυπηρετητή και η απομακρυσμένη κλήση διαδικασιών (RPC), που συνεχίζει να επικρατεί μέχρι και σήμερα στις περισσότερες υπηρεσίες του διαδικτύου.

Στις αρχές της δεκαετίας του 90' Οι Stamos και Gifford συνδύασαν την τεχνολογία RPC με την ιδέα της εκτέλεσης μηνυμάτων, δημιουργώντας την έννοια της απομακρυσμένης αξιολόγησης (Remote evaluation). Η βασική ιδέα ήταν ότι εκτός από τις παραμέτρους, μια διαδικασία να περνά στον εξυπηρετητή και τον κώδικα της που είναι προς εκτέλεση.

Το 1994 η εταιρία General Magic παρουσίασε ένα περιβάλλον και μια γλώσσα προγραμματισμού για συγγραφή και εκτέλεση απομακρυσμένου κώδικα, την πλατφόρμα Telescript και χρησιμοποίησε για πρώτη φορά τον όρο "mobile agents". Η Telescript ήταν ιδικά σχεδιασμένη για τον προγραμματισμό mobile agent και περιελάβανε τις περισσότερες έννοιες των μεταγενέστερων mobile agent συστημάτων.

Από εκεί και έπειτα αναπτύχθηκαν πολλά συστήματα mobile agents κυρίως σε ερευνητικό επίπεδο όπου βασιζόντουσαν σε διάφορες γλώσσες προγραμματισμού, όπως για παράδειγμα η πλατφόρμα Agent Tcl. Σήμερα οι περισσότερες πλατφόρμες βασίζονται στην γλώσσα

προγραμματισμού Java [9]. Μερικά παραδείγματα είναι οι πλατφόρμες Aglets [8], JADE και SeMoA [4].

Αργότερα, υπήρξε η ανάγκη δημιουργίας ορισμένων προτύπων για την υποστήριξη της διαλειτουργικότητας μεταξύ πλατφορμών. Ο στόχος των προτύπων αυτών, ήταν να δώσει την δυνατότητα στους mobile agents, να επικοινωνούν μεταξύ τους για την επιτυχή και γρήγορη εκτέλεση του κώδικά τους, ανεξαρτήτως πλατφόρμας. Τα διασημότερα πρότυπα για mobile agents είναι το FIPA (1996) και το OMG-MASIF (1997) [10].

Στόχος του οργανισμού FIPA (Foundation for Intelligent Physical Agents), ήταν να δημιουργήσει πρότυπα λογισμικού για την ανομοιογενή αλληλεπίδραση και την διαλειτουργικότητα των mobile agents αλλά και των πλατφορμών. Αυτή την στιγμή είναι το επικρατέστερο πρότυπο για την συγκεκριμένη τεχνολογία.

Η OMG (Object Management Group) με το πρότυπο MASIF (Mobile Agent System Interoperability Facilities), ακολούθησε τους στόχους που έθεσε ο FIPA σε ότι αφορούσε το κομμάτι της διαλειτουργικότητας και την υποστήριξη της ανομοιογένειας. Η μεγάλη τους διαφορά όμως βρίσκεται στους στόχους που αφορούν τις απαιτήσεις και τις λειτουργείες των mobile agents. Το πρότυπο αυτό εστιάζει στον τρόπο μεταγωγής του πράκτορα, καθώς επίσης στον τρόπο με τον οποίο μπορεί να δημιουργηθεί δυναμικά.

2.2 Η ασφάλεια των mobile agents / Τύποι επιθέσεων

Στη διεθνή βιβλιογραφία γίνεται εκτενής αναφορά στα θέματα ασφάλειας που κάνουν τους mobile agents (πράκτορες) αλλά και τις πλατφόρμες (πρακτορεία) που εκτελούν τον κώδικά τους ευάλωτες σε διάφορες επιθέσεις. Μπορούν να προσδιορισθούν πέντε τύποι επιθέσεων [1 - 4]:

- Επίθεση από πράκτορα σε πρακτορείο.
- Επίθεση από πρακτορείο σε πράκτορα.
- Επίθεση από πράκτορα σε άλλο πράκτορα.
- Επίθεση από πρακτορείο σε πρακτορείο.
- Επίθεση από έναν εξωτερικό παράγοντα σε πράκτορες ή πρακτορεία.

Ενδεικτικά αναφέρουμε μερικές από τις επιθέσεις [3,4]:

Από κακόβουλο πράκτορα σε πρακτορείο:

- Η μεταμφίεση τους σε εξουσιοδοτημένους πράκτορες.
- Επιθέσεις τύπου DoS (Denial of Service).
- Μη εξουσιοδοτημένη πρόσβαση σε πόρους.
- Αποκήρυξη. Άρνηση δηλαδή του πράκτορα ότι εκτέλεσε συγκεκριμένο κώδικα στο πρακτορείο.

Από κακόβουλο πρακτορείο σε πράκτορα:

- Υποκλοπή ή αλλαγή των δεδομένων
- Καθυστέρηση ή εμπόδιση εκτέλεσης του κώδικα
- Αλλαγή της συμπεριφοράς του (π.χ. κάνοντας τον κακόβουλο)

Από κακόβουλο πράκτορα σε πράκτορα:

- Αλλαγή της κατάστασης εκτέλεσης του.
- Υποκλοπή ή αλλαγή των δεδομένων που φέρει, από μεταμφιεσμένους πράκτορες.
- Εμπόδιση εκτέλεσης του κώδικα.
- Επιθέσεις τύπου DoS λαμβάνοντας πολλά μνήματα spam

Από κακόβουλο πρακτορείο (ή εξωτερικό παράγοντα) σε πρακτορείο και πράκτορες:

- Υποκλοπή επικοινωνίας μεταξύ άλλων πρακτορείων (Επίθεση Man In The Middle)
- Ανάλυση κίνησης και συμπεριφοράς μεταξύ άλλων πρακτορείων με σκοπό την κατάστρωση σχεδίου επίθεσης

Αν και στην μελέτη τους οι Hind Idrissi, El Mamoun Souidi και Arnaud Revel [2], δεν αναφέρονται στους εξωτερικούς παράγοντες που απειλούν ένα πρακτορείο και τους πράκτορες του, είναι ένα σημαντικό ζήτημα που πρέπει να λάβουμε υπόψη.

Οι λύσεις που προτείνονται στα παραπάνω προβλήματα μπορούν να είναι είτε οργανωτικές ή τεχνικές [4]. Και στις δύο περιπτώσεις θα μας βοηθήσουν οι απαιτήσεις του προτύπου ISO 27001 σε μεγάλο βαθμό.

Οργανωτικές λύσεις:

- Να υπάρχει ένα ανεξάρτητο σύστημα αξιολόγησης πρακτορείων και να γίνεται αποδοχή μόνο πρακτόρων που προέρχονται μόνο από πρακτορεία με «καλή φήμη»
- Σύναψη συμβολαίων μεταξύ πρακτορείων με την έγγραφη δέσμευση/εγγύηση ότι το ένα πρακτορείο δεν θα επιτίθεται, χειραγωγεί ή κατασκοπεύει το άλλο.

Τεχνικές λύσεις:

- Χρήση κρυπτογραφίας στα δεδομένα που μεταφέρει ένας πράκτορας.
- Χρήση ψηφιακών υπογραφών και πιστοποιητικών (PKI) για παροχή αυθεντικοποίησης μεταξύ πρακτόρων και πρακτορείων.
- Η εκτέλεση του κώδικα κάθε πράκτορά να γίνεται σε ελεγχόμενο περιβάλλον (sandbox).
- Να υπάρχει ασφαλής δίαυλος επικοινωνίας μεταξύ πρακτορείων (π.χ. χρήση SSL/TLS)
- Να υπάρχει ένα σύστημα έγκαιρης ανίχνευσης επιθέσεων (π.χ. ένα ιδικό IDS)

2.3 Σύγκριση διάσημων πλατφορμών ως προς την ασφάλεια τους

Στις μελέτες τους οι Axel Bürkle, Alice Hertel, Wilmuth Müller και Martin Wieser [4] και οι Donies Samet, Farah Barika Ktata και Khaled Ghedira [5] σύγκριναν ορισμένες διάσημες πλατφόρμες πρακτορείων ως προς το επίπεδο ασφάλειας τους, τρέχοντας κάποιους ελέγχους και εικονικές επιθέσεις. Επιπλέον παρουσιάζουν τρόπους αντιμετώπισης ορισμένων προβλημάτων με την εφαρμογή κανόνων και πολιτικών. Όπως για παράδειγμα η χρήση κρυπτογράφησης, η πιστοποίηση πρακτορείων (Trusted Agencies), ο έλεγχος πρόσβασης πρακτόρων, περιορισμοί ως προς την εκτέλεση του κώδικα, περιορισμοί ως την δημιουργία και κλωνοποίηση πρακτόρων αλλά και την διαχείριση των πόρων του εκάστοτε πρακτορείου.
Στον πίνακα που ακολουθεί γίνεται μια σύγκριση ορισμένων διάσημων πλατφορμών ως προς την ασφάλεια τους. Δίνεται έμφαση στις απαιτήσεις ασφαλείας για διασφάλιση των: διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας.

Πλατφόρμα	Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα
Aglets	Αυθεντικοποίηση: Ναι Κρυπτογράφηση: Ναι Έλεγχος Πρόσβασης: Ναι	Κώδικα: Ναι, μέσω της επέκτασης SAglet Δεδομένων: Όχι	Προστασία μέσω ελέγχου χρήσης πόρων του συστήματος (CPU, RAM, διάρκεια ζωής mobile agent)

SOMA	Αυθεντικοποίηση: Ναι Κρυπτογράφηση: Ναι Έλεγχος Πρόσβασης: Ναι	Κώδικα: Ναι Δεδομένων: Ναι	Προστασία μέσω ελέγχου χρήσης πόρων του συστήματος (CPU, περιορισμός αριθμού λειτουργιών, προτεραιότητα εκτέλεσης, κ.α.)
JADE	Αυθεντικοποίηση: Ναι Κρυπτογράφηση: Ναι Έλεγχος Πρόσβασης: Ναι	Κώδικα: Ναι Δεδομένων: Ναι, μέσω των επεκτάσεων Jade-S & PKI	Προστασία μέσω ελέγχου χρήσης πόρων του συστήματος (μέγιστος χρόνος αναμονής)
Cougaar	Αυθεντικοποίηση: Ναι Κρυπτογράφηση: Ναι Έλεγχος Πρόσβασης: Ναι	Κώδικα: Ναι Δεδομένων: Ναι	Προστασία μέσω ελέγχου χρήσης πόρων του συστήματος (μπλοκάρισμα ports)
SeMoA	Αυθεντικοποίηση: Ναι Κρυπτογράφηση: Ναι Έλεγχος Πρόσβασης: Ναι	Ναι	Ευάλωτη σε επιθέσεις DoS λόγο έλλειψης κατάλληλου ελέγχου των πόρων [14]

Πίνακας 2.1: Σύγκριση διάσημων πλατφορμών mobile agents

2.4 Άλλες προσεγγίσεις για ενίσχυση της ασφάλειας των mobile agents

Γίνονται αρκετές προσπάθειες από ερευνητές, και ανακαλύπτονται συνεχώς νέες μέθοδοι ενίσχυσης της ασφάλειας των mobile agents. Χαρακτηριστική είναι η μέθοδος των Zaki Brahmi, Amine Lini, και Mohamed Mohsen Gammoudi [1] που προτείνουν την χρήση ενός τεχνητού ανοσοποιητικού συστήματος για mobile agents που βασίζεται σε τεχνικές DNA, κρυπτογράφησης και κατακερματισμού, που τους προστατεύουν κατά την διάρκεια της μεταγωγής τους και διασφαλίζουν την επαλήθευση τους στο πρακτορείο προορισμού.

Οι Jean Tajer, Mo Adda και Benjamin Aziz [16] προτείνουν ένα μοντέλο έμπιστων host όπου τα δεδομένα που συλλέγει ο κάθε mobile agent δεν μεταφέρονται στον επόμενο host αλλά μεταφέρονται προσωρινά σε έναν Trusted Server κρυπτογραφημένα με αλγόριθμο κρυπτογράφησης δημοσίου κλειδιού (RSA) και στην συνέχεια μεταφέρονται όλα μαζί στον αρχικό host όπου γίνεται η αποκρυπτογράφηση και η εμφάνιση των αποτελεσμάτων. Με αυτόν τον τρόπο δεν δίνει περιθώριο σε άλλους host να επέμβουν ή να υποκλέψουν πληροφορίες που έχουν συλλεγεί. Ένα αρνητικό στοιχείο αυτής της προσέγγισης είναι ο μεγάλος χρόνος διεκπεραίωσης της εργασίας (περίπου τέσσερις φορές μεγαλύτερος).

Επίσης, στην μελέτη των Hind Idrissi, El Mamoun Souidi και Arnaud Revel [2] προτείνεται μια διαδικασία αυθεντικοποίησης που είναι ανθεκτική σε επιθέσεις τύπου Man In The Middle και που βασίζεται στο πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman σε συνδυασμό με έλεγχο προσπέλασης που βασίζεται στο μοντέλο DAC (Discretionary Access Control).
Επιπλέον, γίνονται και μελέτες που αφορούν την εφαρμογή κάποιων κανόνων ασφάλειας πριν την υλοποίηση των mobile agents. Στην μελέτη τους οι Héla Hachicha, Donies Samet και Khaled Ghedira [3], προτείνουν ένα μοντέλο (βασισμένο στην γλώσσα UML) όπου οι απαιτήσεις ασφάλειας καθορίζονται κατά την φάση του σχεδιασμού τους.

2.5 Το διεθνές πρότυπο ISO 27001

Το ISO 27001 [6] είναι ένα διεθνές πρότυπο που παρέχει τις απαιτήσεις για την εγκαθίδρυση, υλοποίηση, διατήρηση και την συνεχή βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ΣΔΑΠ). Η λειτουργία του ΣΔΑΠ επηρεάζεται από τις ανάγκες και τους στόχους, τις απαιτήσεις ασφάλειας, τις διαδικασίες αλλά και το μέγεθος του οργανισμού που το υλοποιεί.
Σκοπός ενός ΣΔΑΠ είναι να διατηρήσει μέσα από την εφαρμογή μιας διαδικασίας διαχείρισης κινδύνων την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών που διαχειρίζεται ένας οργανισμός. Με αυτόν τον τρόπο δίνει σε όλα τα ενδιαφερόμενα μέρη την αυτοπεποίθηση ότι οι κίνδυνοι έχουν διαχειριστεί επαρκώς.
Ένα σημαντικό πλεονέκτημά του ISO 27001 είναι και το γεγονός ότι ένας οργανισμός που συμμορφώνεται πλήρως με τις απαιτήσεις του, έχει την δυνατότητα να πιστοποιηθεί από φορείς πιστοποίησης, μετά από την διενέργεια επιθεώρησης στο ΣΔΑΠ του. Η πιστοποίηση με την σειρά της, δίνει ένα επιπλέον πλεονέκτημα σε ότι έχει να κάνει με την αγορά και τον ανταγωνισμό που υπάρχει. Δίνει στον οργανισμό δηλαδή ένα συγκριτικό πλεονέκτημα σε σχέση με οργανισμούς που μπορεί να διατηρούν ένα ΣΔΑΠ, αλλά δεν είναι πιστοποιημένοι.
Η έρευνα που διεξάγει κάθε χρόνο ο διεθνής οργανισμός τυποποίησης (ISO) έδειξε ότι το 2017 οι πιστοποιήσεις οργανισμών κατά το πρότυπο ISO 27001 αυξήθηκαν σε παγκόσμια κλίμακα κατά 33,704 σε σχέση με το 2006 και κατά 6,211 (19%) σε σχέση με το 2016. Τα δεδομένα έχουν συλλεγεί από φορείς πιστοποίησης μου είναι μέλη του International Accreditation Forum (IAF). Ακολουθεί το γράφημα που δείχνει τον αριθμό των ενεργών πιστοποιητικών τις χρονιές 2006 – 2017:

Γράφημα 2.1: Ενεργά πιστοποιητικά ISO 27001 (2006-2017)

Ένα κομμάτι τις έρευνας που μας έκανε εντύπωση, είναι το γεγονός ότι το συγκεκριμένο πρότυπο εφαρμόζεται από ένα ευρύ φάσμα βιομηχανικών τομέων, όπως για παράδειγμα εταιρίες που ασχολούνται με την υλοτομία, την γεωργία/αλιεία, αλλά και με εταιρίες που ασχολούνται με πυρηνικά καύσιμα (π.χ. απεμπλουτισμένο ουράνιο) [31, 32]. Το γεγονός αυτό δείχνει την ανάγκη που υπάρχει σε όλους τους τομείς της βιομηχανίας τα τελευταία χρόνια, για την ασφάλεια των πληροφοριών τους.

Μερικές από τις απαιτήσεις του ISO 27001 είναι και ο καθορισμός πολιτικών ασφαλείας πληροφοριών, οι οποίοι πρέπει να εγκριθούν από την διοίκηση του οργανισμού και να κοινοποιηθούν σε όλους τους ενδιαφερόμενους εντός ή εκτός του οργανισμού (Control A.5.1.1). Οι πολιτικές αυτές πρέπει να αναθεωρούνται ανά τακτά διαστήματα για τυχόν αλλαγές που πρέπει να γίνουν ώστε να διασφαλιστεί η επιτηδειότητα, επάρκεια και αποτελεσματικότητά τους (Control A.5.1.1). Επίσης, όλοι οι εμπλεκόμενοι πρέπει να λαμβάνουν κατάλληλη και τακτική εκπαίδευση και να ενημερώνονται σε θέματα που αφορούν τις πολιτικές ασφαλείας που είναι σχετικές με την λειτουργία της εργασίας τους (Control A.7.2.2).

Ένα παράδειγμα μιας τέτοιας πολιτικής ασφαλείας που αφορά την υλοποίηση και χρήση mobile code στα πληροφοριακά συστήματα της Ευρωπαϊκής Επιτροπής αποτελεί το έγγραφο «Standard on mobile code» [7].

Επιπλέον, το ISO 27001 μέσω των 114 ελέγχων ασφάλειας που παρέχεται μαζί με το πρότυπο (στο Annex A), δίνει έμφασή μεταξύ άλλων και στην φυσική ασφάλεια των περιουσιακών στοιχείων του οργανισμού.

Η τελευταία έκδοση του προτύπου (ISO 27001:2013) αποτελείται από τις παρακάτω ενότητες:

0. Εισαγωγή (Introduction)
1. Πεδίο εφαρμογής (Scope)
2. Παραπομπές (Normative references)
3. Όροι και ορισμοί (Terms and definitions)
4. Πλαίσιο λειτουργίας του οργανισμού (Context of the organization)
5. Ηγεσία (Leadership)
6. Σχεδιασμός (Planning)
7. Υποστήριξη (Support)
8. Λειτουργία (Operation)
9. Αξιολόγηση της απόδοσης (Performance evaluation)
10. Βελτίωση (Improvement)
11. Παράρτημα Α – Έλεγχοι Ασφαλείας (Annex A - Controls)

Οι τέσσερις πρώτοι παράγραφοι (0-3) δεν αποτελούν απαιτήσεις, αλλά γενικές πληροφορίες που αφορούν το πρότυπο, το πεδίο εφαρμογής του, παραπομπές, όροι και ορισμοί. Στο Κεφάλαιο 3 θα υλοποιήσουμε τις απαιτήσεις του προτύπου, δηλαδή από την παράγραφο 4 έως την παράγραφο 10 και το Παράρτημα Α.

2.6 Η εξέλιξη των προτύπων της οικογένειας ISO 27000

Την δεκαετία του 90’ το υπουργείο εμπορίου του Ηνωμένου Βασιλείου, εκδήλωσε την ανάγκη να γίνει μια καταγραφή υπό την μορφή οδηγού, καλών πρακτικών και ελέγχων που θα αφορούσαν την ασφάλεια πληροφοριών στον τομέα του εμπορίου και της κυβέρνησης.

Ακολουθεί το χρονικό της εξέλιξης [11, 12]:

- Τον Σεπτέμβριο του 1992 με την βοήθεια κάποιων εταιριών και του BSI (British Standard Institute), δημιουργήθηκε ένας οδηγός καλών πρακτικών υπό μορφή δημοσιεύματος. Ο οδηγός αυτός αποτέλεσε την βάση του Βρετανικού πρότυπου BS 7799-1 που εκδόθηκε το 1995 από το BSI.
- Το 1998 εκδόθηκε το πρότυπο BS 7799-2:1998 το οποίο αποτελούσε μοντέλο για την πιστοποίηση του ΣΔΑΠ οργανισμών.

- Το 1999 εκδόθηκαν οι νέες εκδόσεις των BS 7799-1 και BS 7799-2, που περιλάμβαναν νέους ελέγχους ασφαλείας αλλά και την διαγραφή ορισμένων αναφορών που αφορούσαν το Ηνωμένο Βασίλειο, προετοιμάζοντας με αυτό τον τρόπο το έδαφος για την δημιουργία ενός διεθνούς προτύπου.
- Το 2000 το BS 7799-1 αναδημοσιεύτηκε αλλά αυτή την φορά την μορφή διεθνούς προτύπου το ISO 17799:2000. Το BS 7799-1 και το ISO 17799:2000 συνέχισαν να αναπτύσσονται παράλληλα.
- Το 2002 εκδόθηκε η νέα έκδοση του BS 7799-2 που ενσωμάτωνε μεταξύ άλλων το μοντέλο Plan-Do-Check-Act (PDCA).
- Το 2005 δημοσιεύτηκε από τον Διεθνή Οργανισμό Τυποποίησης (ISO) το διεθνές πρότυπο ISO 27001:2005 το οποίο αντικαθιστούσε το BS7799-2 και περιλάμβανε τους ελέγχους ασφαλείας του ISO 17799 υπό μορφή παραρτήματος (το Annex A).
- Το 2007 δημοσιεύτηκε το 27002:2005 το οποίο θα αντικαταστήσει το ISO 17799. Επίσης θα εκδοθεί και το ISO 27006:2007 το οποίο περιλαμβάνει τις απαιτήσεις για τους φορείς πιστοποίησης που διενεργούν τις επιθεωρήσεις των ΣΔΑΠ των οργανισμών που επιθυμούν πιστοποίηση.
- Το 2008 δημοσιεύεται το ISO 27005:2008 που αφορά την διαχείριση των ρίσκων και το ISO 27011:2008 που αποτελεί οδηγό διαχείρισης ασφάλειας πληροφοριών για εταιρίες τηλεπικοινωνιών και το οποίο είναι βασισμένο στο ISO 27002.
- Το 2009 δημοσιεύονται τα ISO 27000:2009 (διαχείριση ασφάλειας πληροφοριών - επεξήγηση όρων), ISO 27004:2009 (διαχείρισης ασφάλειας πληροφοριών – μετρήσεις) και ISO 27033-1:2009 (ασφάλεια δικτύων - έννοιες).
- Το 2010 δημοσιεύονται τα ISO 27003:2010 (οδηγός υλοποίησης ΣΔΑΠ) και ISO 27033-3:2010 (ασφάλεια δικτύων – σενάρια, απειλές, τεχνικές σχεδιασμού, θέματα που αφορούν τους έλεγχος ασφάλειας).
- Το 2011 δημοσιεύονται οι νέες εκδόσεις των ISO 27005, ISO 27006. Επιπλέον εκδίδονται και τα ISO 27007:2011 (οδηγίες επιθεώρησης ΣΔΑΠ) και ISO 27008:2011 (οδηγίες επιθεώρησης ελέγχων ασφαλείας ΣΔΑΠ).
- Το 2012 δημοσιεύεται η νέα έκδοση του ISO 27000
- Το 2013 δημοσιεύονται οι νέες εκδόσεις των ISO 27001 και ISO 27002
- Το 2014 δημοσιεύεται η νέα έκδοση του ISO 27000
- Το 2015 δημοσιεύεται η νέα έκδοση του ISO 27006
- Το 2016 δημοσιεύονται οι νέες εκδόσεις των ISO 27000 και ISO 27004
- Το 2017 δημοσιεύονται οι νέες εκδόσεις των ISO 27003 και ISO 27007

- Το 2018 δημοσιεύονται οι νέες εκδόσεις των ISO 27000 και ISO 27005

Παρακολουθώντας το πιο πάνω χρονικό του προτύπου μπορούμε εύκολα να καταλήξουμε στο συμπέρασμα ότι το ISO 27001 είναι ένα πρότυπο το οποίο εξελίσσετε και προσαρμόζεται συνεχώς, με σκοπό να ικανοποιήσει τις αυξημένες ανάγκες των οργανισμών για ασφάλεια των πληροφοριών τους από διάφορες απειλές.

2.7 Η υλοποίηση του ISO 27001

Όπως είδαμε στην προηγούμενη ενότητα, το ISO 27001 υιοθέτησε το μοντέλο PDCA (Plan, Do, Check, Act ή Σχεδιασμός, Εκτέλεση, Έλεγχος, Δράση) το οποίο εφαρμόζεται στην δομή όλων των διαδικασιών στο σύστημα διαχείρισης. Σε αυτό το μοντέλο η έξοδος του κάθε στοιχείου τροφοδοτεί την είσοδο του αμέσως επόμενου [19]. Συνοπτικά:

- **Σχεδιασμός** (Εγκαθίδρυση του ΣΔΑΠ): Εγκαθίδρυση των πολιτικών ασφαλείας, των στόχων, των διεργασιών και διαδικασιών που σχετίζονται με την διαχείριση του ρίσκου και η έγκριση τους από την διοίκηση του οργανισμού.
- **Εκτέλεση** (Υλοποίηση του ΣΔΑΠ): Υλοποίηση και λειτουργία των πολιτικών ασφαλείας , των ελέγχων ασφαλείας, των διεργασιών και διαδικασιών που σχετίζονται με το σύστημα διαχείρισης.
- **Έλεγχος** (Παρακολούθηση και ανασκόπηση του ΣΔΑΠ): Παρακολούθηση της απόδοσης των πολιτικών ασφαλείας και των στόχων. Αναφορά με τα αποτελέσματα πρέπει να δίνεται στην διοίκηση για ανασκόπηση και την λήψη αποφάσεων.
- **Δράση** (Διατήρηση και βελτίωση του ΣΔΑΠ): Λήψη προληπτικών και διορθωτικών μέτρων βάση των τακτικών εσωτερικών επιθεωρήσεων και της ανασκόπησης της διοίκησης. Μετά από αυτό το στάδιο η διαδικασία επαναλαμβάνεται από την αρχή.

Αν και υπάρχουν αρκετές προσεγγίσεις και μεθοδολογίες για την υλοποίηση ενός ΣΔΑΠ (όπως για παράδειγμα τα: ISO 10006, PMBOK και IMS2), το 2010 δημοσιεύτηκε από τον Διεθνή Οργανισμό Τυποποίησης το πρότυπο ISO 27003, ένας οδηγός υλοποίησης ειδικά για Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών, όπως ορίζεται στο πρότυπο ISO 27001.
Το πρότυπο, καθοδηγεί τον χρήστη στην αποτελεσματική υλοποίηση του συστήματος. Έχει την δομή και ακολουθεί τις ενότητες του ISO 27001, ενώ δίνει έμφαση στις παρακάτω φάσεις υλοποίησης:

- Κατανόηση των αναγκών του οργανισμού και την αναγκαιότητα δημιουργίας πολιτικών ασφαλείας πληροφοριών, όπως επίσης και ο καθορισμός των στόχων που αφορούν την ασφάλεια πληροφοριών.
- Εκτίμηση των κινδύνων του οργανισμού που σχετίζονται με την ασφάλεια των πληροφοριών.
- Υλοποίηση και λειτουργία διαδικασιών, ελέγχων και άλλων μετρήσεων για μετριασμό των κινδύνων.
- Παρακολούθηση και ανασκόπηση της αποτελεσματικότητας του ΣΔΑΠ.
- Συνεχής βελτίωση.

Κεφάλαιο 3

Υλοποίηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών

3.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα ασχοληθούμε με την υλοποίηση του συστήματος διαχείρισης πληροφοριών (ΣΔΑΠ) για οργανισμούς που ασχολούνται με την παροχή υπηρεσιών και την ανάπτυξη εφαρμογών σε περιβάλλον mobile agents.
Τοποθετήσαμε δηλαδή τα πρακτορεία και τους πράκτορες μέσα στο πλαίσιο ενός οργανισμού. Για τον σκοπό αυτό χρειάστηκε να δημιουργήσουμε έναν οργανισμό-μοντέλο ώστε να μπορέσουμε να καλύψουμε όλες τις απαιτήσεις του προτύπου ISO 27001.
Οι κτιριακές εγκαταστάσεις, η τοπολογία του δικτύου και το οργανόγραμμα του οργανισμού που ακολουθεί στις παρακάτω παραγράφους, περιορίζονται στα βασικά και απολυτός αναγκαία συστατικά.

3.2 Μεθοδολογία υλοποίησης του ΣΔΑΠ

Στον πίνακα που ακολουθεί καθορίζονται τα βήματα που ακολουθήσαμε για την εγκαθίδρυση/υλοποίηση του ΣΔΑΠ σύμφωνα με τις απαιτήσεις του πρότυπου ISO 27001. Όπου χρειάστηκε δημιουργήσαμε τις κατάλληλες τεκμηριωμένες πληροφορίες (έγγραφα και φόρμες), ώστε να υπάρχει συμμόρφωση με το πρότυπο. Έγινε μελέτη της κάθε παραγράφου – απαίτησης του πρότυπου ISO 27001:2013. Σαν οδηγό χρησιμοποιήσαμε το ISO 27003:2017 και ορισμένες πληροφορίες από την ιστοσελίδα ISO 27001 Academy [17] και ESET Cybersecurity Awareness Training [41]. Θεωρούμε ότι το όλο έργο έχει εγκριθεί από την διοίκηση του οργανισμού και ότι έχει αποδεσμευτεί το σχετικό κονδύλι για την υλοποίηση και εφαρμογή του.

Ακολουθούν τα βήματα:

Βήμα	Παράγραφος ISO 27001
1	4.1 – Κατανόηση του οργανισμού και του πλαισίου λειτουργίας του
2	4.2 – Κατανόηση των αναγκών και προσδοκιών των ενδιαφερόμενων μερών
3	4.3 – Καθορισμός πεδίου εφαρμογής του ΣΔΑΠ
4	4.4 – Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
5	5.1 – Ηγεσία και Δέσμευση
6	5.2 – Πολιτική Ασφαλείας
7	5.3 – Οργανωτικοί ρόλοι, ευθύνες και εξουσίες
8	6.1 – Ενέργειες αντιμετώπισης κινδύνων και αξιοποίησης ευκαιριών (Αξιολόγηση & Αντιμετώπιση)
9	Υλοποίηση πολιτικών και διαδικασιών ασφαλείας λαμβάνοντας υπόψιν τους ελέγχους του Παραρτήματος Α (Annex A)
10	Συμπλήρωση της δήλωσης εφαρμοσιμότητας (SoA)
11	6.2 – Στόχοι ασφάλειας πληροφοριών και σχεδιασμός για επίτευξή τους
12	7.1 - Πόροι
13	7.2 – Επαγγελματική επάρκεια
14	7.3 – Ευαισθητοποίηση
15	7.4 - Επικοινωνία
16	7.5 – Τεκμηριωμένες πληροφορίες
17	8.1 – Σχεδιασμός, λειτουργία και έλεγχος των διεργασιών
18	9.1 – Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση
19	9.2 – Εσωτερική επιθεώρηση
20	9.3 – Ανασκόπηση διοίκησης
21	10.1 – Μη συμμόρφωση και διορθωτικές ενέργειες
22	10.2 – Συνεχής βελτίωση

Πίνακας 3.1: Βήματα υλοποίησης ΣΔΑΠ

3.2.1 Κατανόηση του οργανισμού και του πλαισίου λειτουργίας του (Παράγραφος 4.1)

Στην παράγραφο 4.1, το πρότυπο απαιτεί από τον οργανισμό να προσδιορίσει τα εξωτερικά και εσωτερικά ζητήματα που σχετίζονται με τις δραστηριότητες του και που επηρεάζει την δυνατότητα του να πετύχει τα επιδιωκόμενα αποτελέσματα του ΣΔΑΠ. Αυτά τα ζητήματα μπορεί να είναι:

Εξωτερικά ζητήματα:

1. Ανταγωνισμός από άλλους οργανισμούς με παρόμοια δραστηριότητα.

2. Νομικά ζητήματα. Για παράδειγμα η μη συμμόρφωση με το γενικό κανονισμό για τα προσωπικά δεδομένα (GDPR).
3. Φυσικές καταστροφές όπως πυρκαγιά, πλημύρα, σεισμός.
4. Κυβερνοεπιθέσεις.

Εσωτερικά ζητήματα:

1. Η κουλτούρα που καλλιεργείται εντός του οργανισμού.
2. Η έλλειψη στόχων και στρατηγικών του οργανισμού που αφορούν την ασφάλεια των πληροφοριών.
3. Η έλλειψη πολιτικών, διαδικασιών και οι διεργασιών ασφαλείας.
4. Η μη υιοθέτηση κάποιου πρότυπου, ή οδηγίας που αφορά την ασφάλεια.
5. Ο μη ξεκάθαρος καθορισμός ρόλων και υπευθυνοτήτων του προσωπικού.
6. Η μη σύναψη συμβολαίων μεταξύ του οργανισμού και άλλων ενδιαφερόμενων μερών. Ένα παράδειγμα συμβολαίου είναι το συμφωνητικό εμπιστευτικότητας (NDA) του οργανισμού με τους υπαλλήλους.
7. Μη διαθέσιμοι πόροι (π.χ. χρήματα, εξοπλισμός, προσωπικό).
8. Η επαγγελματική ανεπάρκεια του προσωπικού.
9. Η έλλειψη κατάλληλων υποδομών.
10. Ακατάλληλο περιβάλλον εργασίας.
11. Αρνητικά αποτελέσματα εσωτερικών επιθεωρήσεων και η μη λήψη διορθωτικών ενεργειών.
12. Αναποτελεσματική αξιολόγηση ή/και μετριασμός των κινδύνων.

3.2.2 Κατανόηση των αναγκών και προσδοκιών των ενδιαφερόμενων μερών (Παράγραφος 4.2)

Στην παράγραφο 4.2 το πρότυπο απαιτεί από τον οργανισμό να προσδιορίσει τα ενδιαφερόμενα μέρη (εξωτερικά και εσωτερικά) που σχετίζονται με τον οργανισμό και που μπορεί να επηρεαστούν ή να επηρεάσουν την λειτουργία του ΣΔΑΠ. Επιπλέον, πρέπει να προσδιοριστούν οι ανάγκες και οι προσδοκίες των μερών αυτών. Οι ανάγκες αυτές μπορεί να είναι:

Εκτός του οργανισμού:

1. Οι πελάτες που έχουν την ανάγκη να προστατεύονται τα προσωπικά τους δεδομένα.
2. Οι υπηρεσίες έκτακτης ανάγκης (πυροσβεστική, αστυνομία, κτλ.) που απαιτούν να υπάρχει το κατάλληλο περιβάλλον για την ασφάλεια των εργαζομένων (φυσική ασφάλεια, πυρασφάλεια, πρώτες βοήθειες, κτλ.).
3. Οι μέτοχοι και οι επενδυτές, οι οποίοι προσδοκούν στην ανάπτυξη ενός ασφαλούς προϊόντος αλλά και στην αύξηση των κερδών τους.
4. Οι προμηθευτές, σύμβουλοι, υπεργολάβοι, κ.α. που έχουν την ανάγκη τήρησης των συμβολαίων με τον οργανισμό.
5. Οι ρυθμιστές και οι νομοθέτες που απαιτούν την τήρηση της νομοθεσίας.
6. Οι εξωτερικοί συνεργάτες που επίσης έχουν την ανάγκη τήρησης των εργασιακών συμβολαίων με τον οργανισμό.

Εντός του οργανισμού:

1. Η διοίκηση που απαιτεί να υπάρχουν υψηλά επίπεδα ασφαλείας του προϊόντος, το προσωπικό να είναι κατάλληλα καταρτισμένο αλλά ταυτόχρονα να δημιουργούνται και οι κατάλληλες συνθήκες για την μείωση του λειτουργικού κόστους του οργανισμού.
2. Οι εργαζόμενοι που απαιτούν να τηρούνται οι όροι των εργασιακών τους συμβολαίων με τον οργανισμό και να υπάρχουν οι κατάλληλες συνθήκες εργασίας.

3.2.3 Καθορισμός πεδίου εφαρμογής του ΣΔΑΠ (Παράγραφος 4.3)

Για τον καθορισμό του πεδίου εφαρμογής του ΣΔΑΠ χρειάζεται να προσδιοριστούν τα όρια (οργανωτικά, τεχνολογικά και φυσικά) και η εφαρμοσιμότητα του συστήματος. Το πεδίο εφαρμογής είναι ένα κείμενο που τεκμηριώνεται σε ξεχωριστό έγγραφο και πρέπει να εγκριθεί επίσημα από την διοίκηση του οργανισμού.

Το πεδίο εφαρμογής μπορεί να διαφέρει από μια υλοποίηση ΣΔΑΠ σε μία άλλη. Για παράδειγμα μπορεί να περιλαμβάνει:

- Την δραστηριότητα του οργανισμού.
- Μια ή περισσότερες υπηρεσίες που παρέχει ο οργανισμός.
- Ένα ή περισσότερα τμήματα του οργανισμού ή/και τοποθεσίες.

Στην περίπτωση του οργανισμού-μοντέλου που δημιουργήσαμε, το πεδίο εφαρμογής του ΣΔΑΠ που καθορίσαμε είναι:

«Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών εφαρμόζεται στην παροχή υπηρεσιών και την ανάπτυξη εφαρμογών mobile agents από το τμήμα ανάπτυξης λογισμικού των κεντρικών γραφείων του Οργανισμού XYZ που εδρεύει στην Κύπρο. Το πεδίο εφαρμογής είναι συγκεκριμένο για τους ρόλους και τα καθήκοντα που εκτελούνται από το προσωπικό του τμήματος. Σύμφωνα με την δήλωση εφαρμοσιμότητας έκδοση 1.0 ημερομηνίας: xx/xx/xxxx»

Κάθε αλλαγή που γίνεται στο πεδίο εφαρμογής, πρέπει να αξιολογείται, να εγκρίνεται και να καταγράφεται.

Η δήλωση εφαρμοσιμότητας (Statement of Applicability ή απλά SoA) που αναφέρεται στο πεδίο εφαρμογής, είναι ένα κείμενο που συντάσσεται σύμφωνα με τα αποτελέσματα της αντιμετώπισης των κινδύνων (risk treatment). Το κείμενο αυτό θεωρείται το προφίλ ασφάλειας του οργανισμού και αποτελείται από τους ελέγχους ασφαλείας που εφαρμοστήκαν σύμφωνα με το Annex A του προτύπου, τον τρόπο με τον οποίο εφαρμόστηκαν αλλά και την τρέχουσα κατάστασή τους. Θα το μελετήσουμε σε επόμενη παράγραφο όταν θα κάνουμε την διαχείριση κινδύνων.

3.2.4 Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Παράγραφος 4.4)

Όπως είδαμε στο Κεφάλαιο 2, Το ISO 27001 είναι ένα πρότυπο που παρέχει τις απαιτήσεις για την εγκαθίδρυση, υλοποίηση, διατήρηση και την συνεχή βελτίωση ενός ΣΔΑΠ. Σύμφωνα με την παράγραφο 4.4, το πρότυπο απαιτεί από τον οργανισμό να συμμορφώνεται με όλες τις απαιτήσεις του ISO 27001, ώστε να εγκαθιδρύσει, να υλοποιήσει, να διατηρήσει και να βελτιώνει συνεχώς το ΣΔΑΠ.

3.2.5 Ηγεσία και Δέσμευση (Παράγραφος 5.1)

Η διοίκηση του οργανισμού πρέπει να επιδεικνύουν ηγεσία και δέσμευση σε ότι αφορά την λειτουργία του ΣΔΑΠ. Αυτό μπορεί να το πετύχει με αρκετούς τρόπους όπως για παράδειγμα:

- Με την ενημέρωση του προσωπικού για την σημαντικότητα του ΣΔΑΠ και τα οφέλη που θα αποκομίσει ο οργανισμός από την εφαρμογή του, όπως η ασφάλεια των ευαίσθητων πληροφοριών, την εμπιστοσύνη των πελατών, την ανταγωνιστικότητα στην αγορά, κ.α.
- Με την παροχή των πόρων που χρειάζονται, ώστε να υλοποιηθεί και να λειτουργήσει το ΣΔΑΠ.
- Με την ενσωμάτωση των απαιτήσεων του ΣΔΑΠ στις καθημερινές δραστηριότητες του οργανισμού.
- Με την επίτευξη των στόχων ασφάλειας που έχουν τεθεί.
- Εκπαιδεύοντας το προσωπικό σε θέματα που αφορούν την ασφάλεια των πληροφοριών.
- Προωθώντας την συνεχή βελτίωση του ΣΔΑΠ.

3.2.6 Πολιτική Ασφαλείας (Παράγραφος 5.2)

Η διοίκηση του οργανισμού πρέπει να καταγράψει και να κοινοποιήσει σε όλα τα ενδιαφερόμενα μέρη μια πολιτική ασφαλείας που περιλαμβάνει στην ουσία την δέσμευση του οργανισμού για την εφαρμογή όλων των απαιτήσεων ασφαλείας του ΣΔΑΠ, τους βασικούς στόχους ασφαλείας του οργανισμού, την δέσμευση για την συνεχή βελτίωση του ΣΔΑΠ.

Στην περίπτωση του οργανισμού-μοντέλου που δημιουργήσαμε, η πολιτική ασφάλειας του οργανισμού είναι:

«Η διοίκηση του οργανισμού XYZ που δραστηριοποιείται στην ανάπτυξη εφαρμογών σε περιβάλλον mobile agent, δεσμεύεται ότι θα διατηρήσει την Εμπιστευτικότητα, την Ακεραιότητα και την Διαθεσιμότητα όλων των φυσικών και ψηφιακών πληροφοριών του οργανισμού, ώστε να διασφαλίσει την ανταγωνιστικότητα, την ροή κεφαλαίου, την κερδοφορία, τις νομικές και ρυθμιστικές υποχρεώσεις του, καθώς και την εμπορική του εικόνα.

Οι απαιτήσεις ασφάλειας των πληροφοριών του οργανισμού θα συνεχίσουν να είναι ευθυγραμμισμένες με συγκεκριμένους στόχους που έθεσε η διοίκηση του.

Το ΣΔΑΠ θα αποτελεί το εργαλείο όπου όλες οι διαδικασίες του θα βελτιώνονται συνεχώς για την επίτευξη των στόχων ασφάλειας, μειώνοντας τους σχετικούς κίνδυνους σε επιτρεπτά όρια.

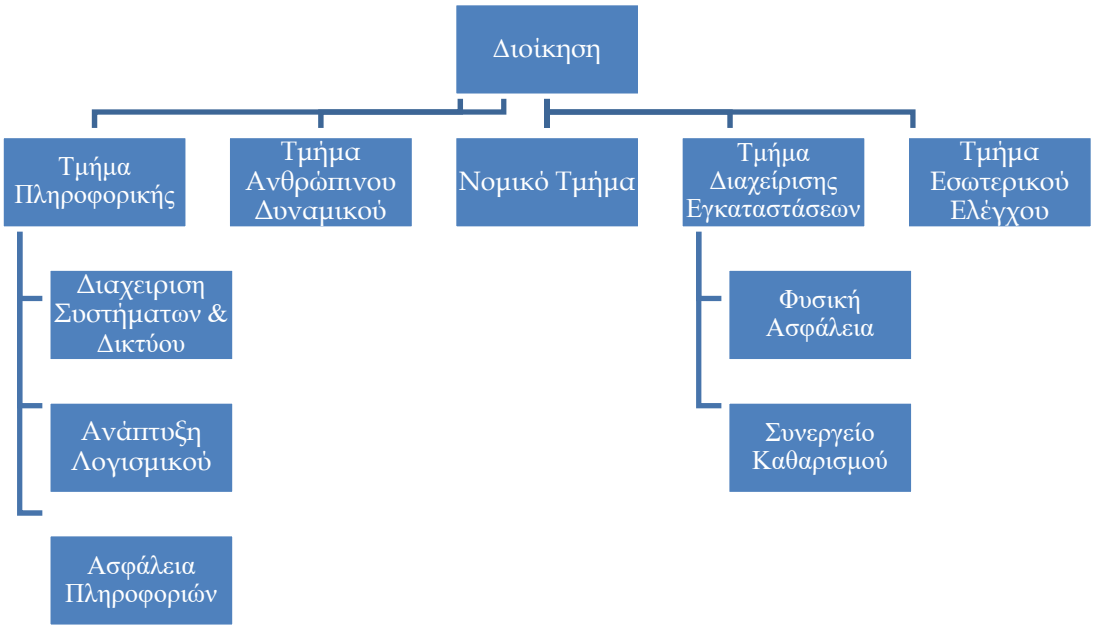
Ο οργανισμός αναμένει από προσωπικό και τους εξωτερικούς συνεργάτες ότι θα συμμορφώνεται με αυτή την πολιτική αλλά και το ΣΔΑΠ που υλοποιεί αυτή την πολιτική. Οι συνέπιες της παραβίασης αυτής της πολιτικής ορίζονται σε σχετική πειθαρχική διαδικασία, στα συμβόλαια και σε συμφωνίες με τρίτους.»

Σε αυτό το σημείο να σημειώσουμε ότι πιο συγκεκριμένοι και μετρήσιμοι στόχοι ασφαλείας θα οριστούν και στην συνέχεια, σύμφωνα με την παράγραφο 6.2 του προτύπου και αφού γίνει η διαδικασία της αξιολόγησης και της αντιμετώπισης των κινδύνων (Παράγραφος 6.1).

3.2.7 Οργανωτικοί ρόλοι, ευθύνες και εξουσίες (Παράγραφος 5.3)

Το πρότυπο στην παράγραφο 5.3 του προτύπου απαιτεί από την διοίκηση του οργανισμού να τεκμηριώσει, να καθορίσει, να εγκρίνει και να αναθέσει ρόλους, ευθύνες και εξουσίες που σχετίζονται με το ΣΔΑΠ και στην συνεχεία να τους κοινοποιήσει στο προσωπικό.

Ακολουθεί το οργανόγραμμα του οργανισμού-μοντέλου που δημιουργήσαμε:



Σχήμα 3.1: Οργανόγραμμα ενός τυπικού οργανισμού που ασχολείται με την ανάπτυξη εφαρμογών

Στην περίπτωση του οργανισμού-μοντέλου που δημιουργήσαμε, οι ρόλοι, οι ευθύνες και οι εξουσίες του οργανισμού είναι:

Τμήμα	**Ρόλος**	**Κύρια Καθήκοντα**
Διοίκηση		• Νόμιμος ιδιοκτήτης των περιουσιακών στοιχείων του οργανισμού. • Καθιέρωση της πολιτικής και τους στόχους ασφαλείας • Ενσωμάτωση των απαιτήσεων του ΣΔΑΠ στις διεργασίες του οργανισμού. • Διασφαλίζει τους απαραίτητους πόρους για το ΣΔΑΠ. • Διασφαλίζει ότι το ΣΔΑΠ πετυχαίνει τους επιδιωκόμενους στόχους. • Καθοδηγεί και υποστηρίζει το προσωπικό (διοικητικό ή μη) που συνεισφέρει στην αποτελεσματικότητα του ΣΔΑΠ. • Προωθεί την συνεχή βελτίωση.
Πληροφορικής	Διευθυντής Πληροφορικής	Συντονισμός δραστηριοτήτων του τμήματος.
Πληροφορικής -> Διαχείριση Συστημάτων & Δικτύου	Διαχειριστής Συστημάτων και Δικτύου	• Παρακολούθηση κίνησης δικτύου. • Παρακολούθηση Antivirus. • Ρύθμιση Firewall. • Ρύθμιση Web Content Filter • Τήρηση και επαλήθευση αντιγράφων ασφαλείας. • Έλεγχος Χωρητικοτήτων (Storage, Network Bandwidth, κτλ.) • Εγκατάσταση/Αναβάθμιση εφαρμογών. • Έλεγχος πρόσβασης στα συστήματα. • Ανάλυση αρχείων καταγραφής (log files). • Καταγραφή , αναφορά και αντιμετώπιση περιστατικών ασφαλείας. • Διασφάλιση απρόσκοπτης παροχής ηλεκτρικού ρεύματος στα συστήματα • Συντήρηση εξοπλισμού υπολογιστικών συστημάτων

		• Έλεγχος δικαιωμάτων πρόσβασης mobile agents άλλων πρακτορείων. • Λήψη ενημέρωσης από έγκυρες πηγές, σχετικά με ευπάθειες των συστημάτων του οργανισμού
Πληροφορικής -> Ανάπτυξη Λογισμικού	Προγραμματιστής	• Ανάπτυξη και έλεγχος ασφαλών εφαρμογών σε πλατφόρμα mobile agent. • Version Control του κώδικα.
Πληροφορικής -> Ασφάλεια Πληροφοριών	Διευθυντής Ασφάλειας Πληροφοριών	• Υλοποίηση του ΣΔΑΠ. • Συνεργασία με τους διευθυντές των άλλων τμημάτων για τον καθορισμό των πολιτικών ασφαλείας. • Συντονισμός και παρακολούθηση δραστηριοτήτων σχετικές με την διαχείριση ασφάλειας πληροφοριών και λειτουργειών του ΣΔΑΠ. • Τυχαίοι δειγματοληπτικοί έλεγχοι συμμόρφωσης του ΣΔΑΠ • Επικοινωνία με το προσωπικό ή τους εξωτερικούς συνεργάτες για θέματα που αφορούν την ασφάλεια δεδομένων. • Λήψη ενημέρωσης από έγκυρες πηγές, σχετικά με ευπάθειες των συστημάτων του οργανισμού. • Ενημέρωση της διοίκησης σχετικά με την απόδοση του ΣΔΑΠ.
Ανθρώπινου Δυναμικού	Διευθυντής Ανθρώπινου Δυναμικού	• Πρόσληψη/Απόλυση Προσωπικού • Υλοποίηση και διαχείριση της εκπαίδευσης και της ευαισθητοποίησης του προσωπικού σε θέματα ασφάλειας. • Επικοινωνία με το προσωπικό για θέματα που αφορούν την εκπαίδευσή τους
Νομικό	Νομικός Σύμβουλος	Προσδιορισμός απαιτήσεων συμμόρφωσης με νόμους, οδηγίες, συμβόλαια, κτλ.).
Διαχείρισης Εγκαταστάσεων	Διευθυντής Διαχείρισης Εγκαταστάσεων	Συντονισμός δραστηριοτήτων του τμήματος.
Διαχείρισης Εγκαταστάσεων	Υπεύθυνος Φυσικής Ασφάλειας	Υλοποίηση και διαχείριση ελέγχων φυσικής ασφάλειας: • σύστημα συναγερμού • περιμετρική ασφάλεια

		• έλεγχος πρόσβασης στις εγκαταστάσεις • πυρασφάλεια • καταστροφή μέσων αποθήκευσης Ζωντανή παρακολούθηση CCTV Συνοδεία ατόμων που δεν ανήκουν στον οργανισμό Συντήρηση εξοπλισμού. Επικοινωνία με το προσωπικό για θέματα που αφορούν την φυσική ασφάλεια ή τις ασκήσεις ετοιμότητας. Λήψη ενημέρωσης από έγκυρες πηγές, σχετικά με ευπάθειες των συστημάτων του οργανισμού
Διαχείρισης Εγκαταστάσεων	Συνεργείο Καθαρισμού	Εξωτερικός συνεργάτης, υπεύθυνος για τον καθαρισμό του κτηρίου.
Εσωτερικού Ελέγχου	Εσωτερικός Ελεγκτής	• Επικύρωση ΣΔΑΠ (Έλεγχος συμμόρφωσης με το πρότυπο). • Να είναι αντικειμενικός και αμερόληπτος. • Ενημέρωση της διοίκησης σχετικά με την συμμόρφωση με το πρότυπο ISO 27001.

Πίνακας 3.2: Οι ρόλοι, οι ευθύνες και οι εξουσίες του οργανισμού

3.2.8 Ενέργειες αντιμετώπισης κινδύνων και αξιοποίησης ευκαιριών (Παράγραφος 6.1)

Ο οργανισμός λαμβάνοντας υπόψιν τα εξωτερικά και εσωτερικά ζητήματα (Παράγραφος 4.1) και τις απαιτήσεις (Παράγραφος 4.2) πρέπει:

- Να αξιολογήσει τους κινδύνους και να αξιοποιήσει τις ευκαιρίες που έχει να αντιμετωπίσει και που σχετίζονται με την ασφάλεια των πληροφοριών.
- Να αντιμετωπίσει αυτούς τους κίνδυνους και να εκμεταλλευτεί τις ευκαιρίες.

Ο λόγοι που το κάνει αυτό ο οργανισμός είναι για να:

- Διασφαλίσει ότι θα επιτευχθούν οι στόχοι που έθεσε (Παράγραφοι 5.2 και 6.2).

- Αποτρέψει ή να μειώσει ανεπιθύμητες επιπτώσεις στα περιουσιακά του στοιχεία.
- Να πετύχει τη συνεχή βελτίωση του ΣΔΑΠ.

Οι ευκαιρίες που μπορεί να εκμεταλλευτεί ένας οργανισμός μπορεί να είναι:

- Η φυσική και η ψηφιακή ασφάλεια των πληροφοριών του οργανισμού.
- Η εκπαίδευση του προσωπικού σε θέματα ασφάλειας πληροφοριών.
- Η παροχή ασφαλών υπηρεσιών / εφαρμογών.
- Στην περίπτωση πιστοποίησης του ΣΔΑΠ από διαπιστευμένο φορέα πιστοποίησης τότε θα έχει το ανταγωνιστικό πλεονέκτημα στην αγορά σε σχέση με άλλους οργανισμούς χωρίς πιστοποιημένο ΣΔΑΠ.

3.2.8Α Αξιολόγηση Κινδύνων (Παράγραφος 6.1.2)

Κατά την διαδικασία αξιολόγησης των κινδύνων ο οργανισμός πρέπει:

- Να καθορίσει τα κριτήρια αποδοχής και αξιολόγησης του κίνδυνου.
- Να διασφαλίσει ότι η επανάληψη της διαδικασίας αξιολόγησης των κινδύνων θα παράγει σταθερά, έγκυρα και συγκρίσιμα αποτελέσματα.
- Να προσδιορίσει τους κίνδυνους που σχετίζονται με την απώλεια της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των περιουσιακών στοιχείων του οργανισμού, αλλά και τους ιδιοκτήτες των κινδύνων αυτών.
- Να αναλύσει τις επιπτώσεις, την πιθανότητα εμφάνισης αλλά και το επίπεδο του κάθε κινδύνου.
- Να κατηγοριοποιήσει τους κινδύνους δίνοντας προτεραιότητα στους πιο σοβαρούς για το επόμενο βήμα που είναι η αντιμετώπιση τους.

Ο οργανισμός πρέπει να διατηρεί καταγεγραμμένα τεκμήρια κατά την διάρκεια όλης της διαδικασίας.

Μεθοδολογία:

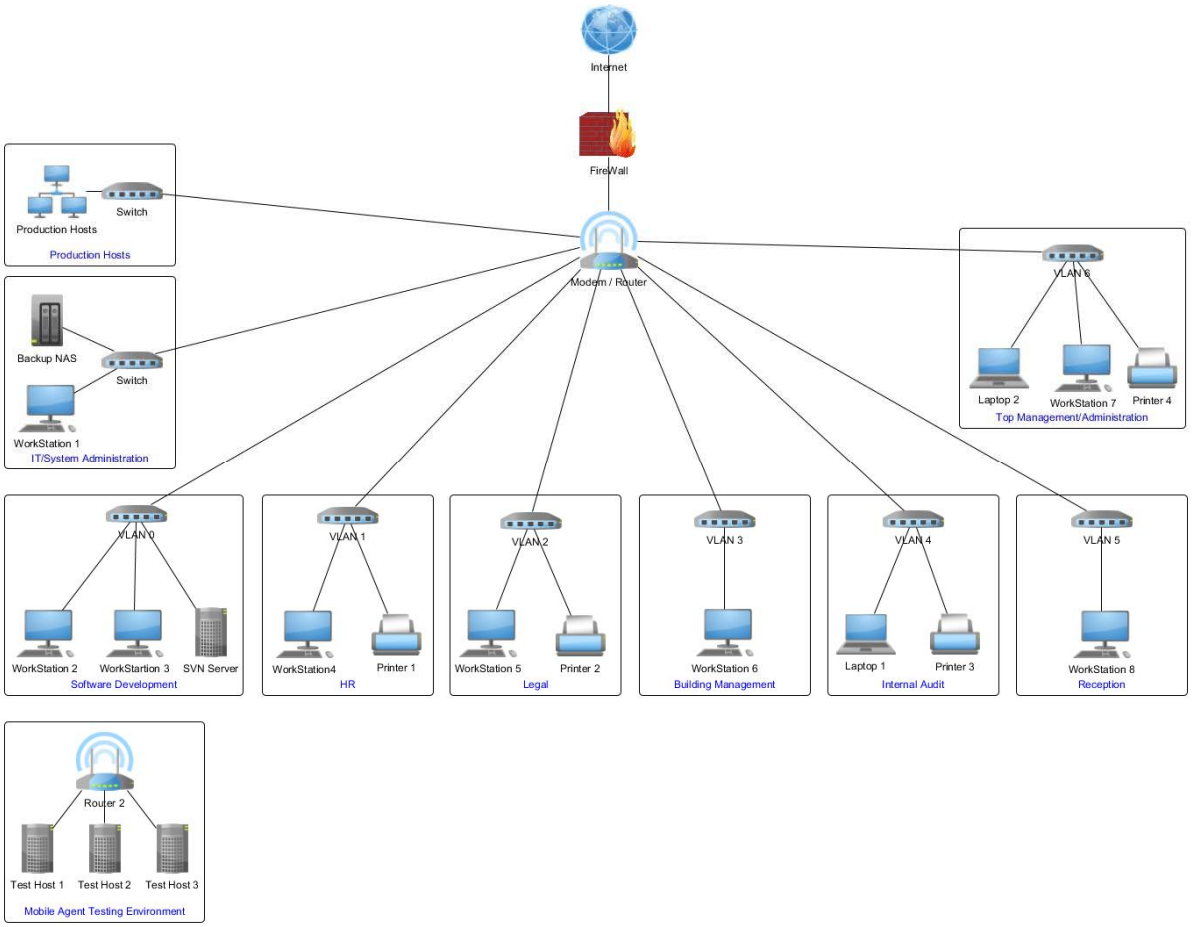
Η μεθοδολογία που θα χρησιμοποιήσουμε για την αξιολόγηση του κινδύνου θα είναι βασισμένη στις ευπάθειες των περιουσιακών στοιχείων του οργανισμού που σχετίζονται με την ασφάλεια

των πληροφοριών (**Παράρτημα Α – Α.1**). Για κάθε περιουσιακό στοιχείο ορίσαμε τον ιδιοκτήτη, και αξιολογήσαμε τον κίνδυνο βάση κάποιων κριτηρίων.

Περιουσιακά στοιχεία του οργανισμού θεωρούνται:

- Όλο το εμπλεκόμενο προσωπικό (εντός ή εκτός του οργανισμού)
- Τα δεδομένα
- Το λογισμικό
- Το υλικό
- Οι διαδικασίες
- Ο δικτυακός εξοπλισμός

Λαμβάνοντας υπόψιν το οργανόγραμμα που ορίσαμε στην παράγραφο 3.2.7, ακολουθούν τα παραδείγματα της τοπολογίας δικτύου (Σχήμα 3.2) καθώς επίσης και των κτιριακών εγκαταστάσεων (Σχήμα 3.3) του οργανισμού-μοντέλου που δημιουργήσαμε. Αυτό θα μας βοηθήσει στην διαχείριση κινδύνων, αλλά και στο να έχουμε μια καλύτερη εικόνα των περιουσιακών στοιχείων του οργανισμού.



Σχήμα 3.2: Η τοπολογία του δικτύου

Κτηριακές Εγκαταστάσεις:

Εικόνα 3.3: Οι κτηριακές εγκαταστάσεις

Ακολουθούν τα κριτήρια που θέσαμε για την αξιολόγηση των κινδύνων:

Κριτήρια Κινδύνου	Περιγραφή
Κριτήριο Επίπτωσης	Κλίμακα: 1-10 (1 – Μικρή Επίπτωση, 10 – Μεγάλη Επίπτωση). Θα οριστεί βάση της ζημιάς που μπορεί να προκαλέσει στον οργανισμό (οικονομική, νομική, φήμης, κτλ.).
Πιθανότητα Εμφάνισης	Κλίμακα: 1-10 (1 – Μικρή Πιθανότητα, 10 – Μεγάλη Πιθανότητα). Θα οριστεί βάση την κρίση και την εμπειρία μας.
Κριτήριο Αξιολόγησης	Κίνδυνος = Επίπτωση * Πιθανότητα Εμφάνισης.
Κριτήριο Αποδοχής	Κίνδυνος <= 60
Κλίμακα	**1-49 Χαμηλός** **50-69 Μέτριος** **70-100 Υψηλός**

Πίνακας 3.3: Τα κριτήρια της αξιολόγησης του κινδύνου

Η εξίσωση που χρησιμοποιήσαμε για την αξιολόγηση του κινδύνου (Κίνδυνος = Επίπτωση * Πιθανότητα Εμφάνισης) μας βοηθά να ποσοτικοποιήσουμε τον κίνδυνο, μιας και έχουμε να κάνουμε με υποκειμενικές τιμές όπως η επίπτωση και η πιθανότητα εμφάνισης. Επιπλέον βοηθά στο να δημιουργήσουμε μια κλίμακα (από 1 – 100) για τον καθορισμό του επιπέδου του κινδύνου. Για παράδειγμα, εάν η επίπτωση ενός κινδύνου είναι υψηλή και δεν εφαρμόσουμε τους κατάλληλους ελέγχους για να μειώσουμε την πιθανότητα εμφάνισης του, τότε ο κίνδυνος θα είναι πολύ υψηλός. Από την άλλη αν εφαρμόσουμε ελέγχους τότε μειώνετε μαζί με την πιθανότητα εμφάνισης και ο κίνδυνος.

Υπάρχουν αρκετές παραλλαγές της εξίσωσης αξιολόγησης, αυτή που χρησιμοποιήσαμε θεωρείτε ότι είναι πιο κοντά στον τρόπο με τον οποίο αντιλαμβάνεται ο άνθρωπος τον κίνδυνο εκ φύσεως. Να σημειώσουμε επίσης ότι η πιθανότητα εμφάνισης, θα είναι πάντα μεγαλύτερη από μηδέν (>0), ανεξαρτήτως των ελέγχων που εφαρμόζουμε, λόγο κυρίως του ανθρώπινου παράγοντα που είναι απρόβλεπτος , αλλά και λόγο της πολυπλοκότητας των περισσότερων συστημάτων (software, hardware, κτλ.) που πάντα θα κρύβουν ευπάθειες. Όσο αφορά τον ανθρώπινο παράγοντα, ενδεικτικά, να αναφέρουμε τις περιπτώσεις των Chelsea Manning και Edward Snowden οι οποίοι κατάφεραν να διαρρεύσουν διαβαθμισμένες - απόρρητες πληροφορίες από εγκαταστάσεις υψίστης ασφαλείας όπως είναι οι μονάδες στρατού και η Υπηρεσία Εθνικής Ασφάλειας (NSA) των ΗΠΑ [39, 40].

Αξιολόγηση Κινδύνων (Παράδειγμα):

Περιουσιακό Στοιχείο	Ιδιοκτήτης	Κίνδυνος	Ευπάθεια	Επίπτωση	Πιθανότητα Εμφάνισης	Κίνδυνος
Mobile Agent	Προγραμματιστής	Διαρροή πληροφοριών	Απώλεια εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	6	**60**
-//-	-//-	Κακόβουλοι agents	Απώλεια διαθεσιμότητας και ακεραιότητας των δεδομένων.	10	6	**60**

Πίνακας 3.4: Αξιολόγηση Κινδύνων (Παράδειγμα)

Η ολοκληρωμένη αξιολόγηση κινδύνων δίνεται στο **Παράρτημα Α (Α.2)**.

3.2.8Β Αντιμετώπιση Κινδύνων (Παράγραφος 6.1.3)

Κατά την διαδικασία της αντιμετώπισης των κινδύνων ο οργανισμός πρέπει:

- Να επιλέξει τον τρόπο με τον οποίο θα αντιμετωπίσει τον κάθε κίνδυνο λαμβάνοντας υπόψιν τα αποτελέσματα της αξιολόγησης των κινδύνων. Οι επιλογές μπορεί να είναι [15]:

    - **Μείωση Κινδύνου** – Εφαρμογή ελέγχων ασφαλείας για την μείωση της πιθανότητας εμφάνισης του κινδύνου. Στο Παράρτημα Α του ISO 27001, υπάρχει μια λίστα με κατηγοριοποιημένους 144 ελέγχους ασφαλείας που πρέπει να εφαρμοστούν ώστε να επιτευχθεί η συμμόρφωση με το πρότυπο. Η μη εφαρμογή κάποιου από τους ελέγχους πρέπει να δικαιολογείται, ενώ επιτρέπεται η εφαρμογή κάποιου ελέγχου που δεν υπάρχει στο Παράρτημα Α.
    - **Αποφυγή Κινδύνου** - Τερματισμός όλων των ενεργειών που μπορεί να προκαλέσουν τον κίνδυνο.
    - **Μεταφορά Κινδύνου** – Μεταφορά του κινδύνου σε άλλο μέρος (π.χ. αγορά υπηρεσιών από τρίτους) .
    - **Διατήρηση Κινδύνου** – Αποδοχή του κινδύνου χωρίς να εφαρμοστεί οποιοσδήποτε έλεγχος. Συνήθως επιλέγουμε αυτή την επιλογή όταν το κόστος αντιμετώπισης του κινδύνου είναι μεγαλύτερο από το κόστος που θα προκαλέσει το περιστατικό ασφαλείας ενός τέτοιου κινδύνου.

- Παραγωγή της «Δήλωσης Εφαρμοσιμότητας» (Statement of Applicability ή SoA) που θα περιλαμβάνει τους ελέγχους που εφαρμόστηκαν από το Παράρτημα Α, όπως επίσης και την δικαιολογία σε περίπτωση εξαίρεσης ενός ελέγχου.
- Δρομολόγηση ενός προγράμματος για την υλοποίηση και εφαρμογή των ελέγχων (Καθορισμός συγκεκριμένων ημερομηνιών) το οποίο θα εγκριθεί και θα εφαρμοστεί από τον ιδιοκτήτη του κινδύνου.

Αντιμετώπιση Κινδύνων (Παράδειγμα):

Περιουσιακό Στοιχείο	**Ευπάθεια**	**Έλεγχοι**	**Κίνδυνος**	**Αντιμετώπιση**	**Ημερομηνία Εφαρμογής Ελέγχων**
Mobile Agents/Data	Διαρροή πληροφοριών	Χρήση Κρυπτογράφησης στα δεδομένα που μεταφέρει ο agent αλλά και στο κανάλι επικοινωνίας (χρήση SSL)	**60**	Μείωση Κινδύνου	1/3/2019
Mobile Agents/Data	Κακόβουλοι agents	**Οργανωτικοί:** Εφαρμογή συστήματος βαθμολόγησης πρακτορείων, Αποδοχή agents μόνο από πρακτορεία καλής φήμης, Σύναψη συμβολαίων μεταξύ πρακτορείων όπου θα απαγορεύει κακόβουλες ενέργειες μεταξύ πρακτορείων (συμφωνία προθέσεων), Κατάθεση Αίτησης με τα στοιχεία του mobile agent και την διαδρομή που θα ακολουθήσει, Τακτικές αμοιβαίες επιθεωρήσεις (π.χ. του κώδικα ή του ISMS) μεταξύ πρακτορείων (2nd ή 3rd Party Audits) **Τεχνικοί:** Εκτέλεση του agent σε ασφαλές περιβάλλον (sandbox), Περιορισμός agents σε πόρους του συστήματος (CPU, RAM, Network, Files, κτλ.), Λήψη εξουσιοδότηση για εκτέλεση κώδικα στον Host, Αυθεντικοποίηση Agent/Host, Έλεγχος ακεραιότητας δεδομένων, Μηχανισμοί μη αποκήρυξης αποστολής/ λήψης/ εκτέλεσης των agents	**60**	Μείωση Κινδύνου	1/3/2019

Πίνακας 3.5: Αντιμετώπιση Κινδύνων (Παράδειγμα)

Η ολοκληρωμένη αντιμετώπιση των κινδύνων δίνετε στο **Παράρτημα Α (Α.3)**. Όπου χρειάστηκε δημιουργήθηκαν οι κατάλληλες πολιτικές ασφαλείας και διαδικασίες, σχεδιασμοί, αρχεία καταγραφής, φόρμες και συμβόλαια. Δίνονται στα **Παραρτήματα Β, Γ, Δ, Ε, Ζ**. Ο πίνακας αντιμετώπισης των κινδύνων πρέπει να ενημερώνετε κάθε φορά που εφαρμόζεται ένας νέος έλεγχος.

Στο **Παράρτημα Η** δίνεται η Δήλωση Εφαρμοσιμότητας (Statement of Applicability).

Για την δημιουργία των πολιτικών χρησιμοποιήσαμε σαν οδηγό την δομή των εγγράφων που ακολουθεί το SANS Institute [18] και που συμμορφώνεται όπως θα δούμε με τις απαιτήσεις του ISO 27001 (Παράγραφος 7.5).

3.2.9 Στόχοι ασφάλειας πληροφοριών και σχεδιασμός για επίτευξή τους (Παράγραφος 6.2)

Σε αυτή την παράγραφο το πρότυπο απαιτεί από τον οργανισμό να καθιερώσει και να τεκμηριώσει τους στόχους του για την ασφάλεια πληροφοριών. Αυτοί οι στόχοι πρέπει:

- Να είναι συνεπείς με την πολιτική ασφαλείας (Παράγραφος 5.2).
- Να είναι μετρήσιμοι.
- Να λαμβάνουν υπόψιν εφαρμόσιμες απαιτήσεις ασφαλείας πληροφοριών και αποτελέσματα της εκτίμησης των κινδύνων.
- Να κοινοποιούνται σε όλα τα ενδιαφερόμενα μέρη.
- Να ενημερώνονται καταλλήλως μόλις προκύψει η ανάγκη για αλλαγή.

Επιπλέον, πρέπει να καταγράφεται ο τρόπος που θα επιτευχθούν οι στόχοι και να καθοριστούν τα παρακάτω:

- Οι ενέργειες που πρέπει να γίνουν.
- Οι πόροι που απαιτούνται.
- Ποιος θα είναι ο υπεύθυνος για την επίτευξή του.
- Πότε πρέπει να ολοκληρωθεί.

- Πως θα γίνεται η αξιολόγηση των αποτελεσμάτων (π.χ. μέσω της διαδικασίας της εσωτερικής επιθεώρησης, τυχαίων δειγματοληπτικών ελέγχων, παρατήρηση, κτλ.).

Στην περίπτωση του οργανισμού-μοντέλου που δημιουργήσαμε οι στόχοι είναι:

#	Παράμετρος	Στόχος	Ενέργεια	Πόροι	Υπεύθυνος	Περιοδικότητα
1	Μη συμμορφώσεις με το πρότυπο ISO 27001	<=3	Εσωτερική επιθεώρηση	Διαθεσιμότητα του εμπλεκόμενου προσωπικού για μια εργάσιμη ημέρα.	Εσωτερικός Ελεγκτής	Κάθε 6 μήνες
2	Μη τήρηση συμφωνιών/ NDA	0	Παρατήρηση	-	Διοίκηση	Κάθε 6 μήνες
3	Επανεμφανίσεις μη συμμορφώσεων με το πρότυπο ISO 27001	0	Εσωτερική επιθεώρηση	Διαθεσιμότητα του εμπλεκόμενου προσωπικού για μια εργάσιμη ημέρα.	Εσωτερικός Ελεγκτής	Κάθε 6 μήνες
4	Εμφανίσεις σοβαρών περιστατικών ασφάλειας	<=2	Παρακολούθηση κατάστασης συστημάτων προστασίας	Αρχεία καταγραφής συστημάτων προστασίας	Διαχειριστής Συστημάτων και Δικτύου / Υπεύθυνος Φυσικής Ασφάλειας	Κάθε 6 μήνες
5	Εμφανίσεις ήπιων περιστατικών ασφάλειας	<=10	Παρακολούθηση κατάστασης συστημάτων προστασίας	Αρχεία καταγραφής συστημάτων προστασίας	Διαχειριστής Συστημάτων και Δικτύου / Υπεύθυνος Φυσικής Ασφάλειας	Κάθε 6 μήνες

6	Περιστατικά εκδήλωσης πυρκαγιάς	0	Τοποθέτηση αυτόματου συστήματος πυρασφάλειας	Έγκληση σχετικού κονδυλίου	Υπεύθυνος Φυσικής Ασφάλειας	Κάθε 6 μήνες
7	Νομικά Ζητήματα	0	Παρακολούθηση και ενημέρωση για νομικά ζητήματα που αφορούν την δραστηριότητα του οργανισμού	-	Διοίκηση / Νομικός Σύμβουλος	Κάθε 6 μήνες
8	Ζητήματα που αφορούν άδειες χρήσης λογισμικού	0	Αγορά νόμιμων αδειών χρήσης λογισμικού	Έγκριση σχετικού κονδυλίου	Διαχειριστής Συστημάτων και Δικτύου	Κάθε 6 μήνες
9	Αποτυχημένες απόπειρες τήρησης αντιγράφου ασφαλείας	<=3	Χρήση σύγχρονου εξοπλισμού (HW & SW)	Έγκριση σχετικού κονδυλίου	Διαχειριστής Συστημάτων και Δικτύου	Κάθε 6 μήνες
10	Διακοπές Ρεύματος (ώρες)	<=4	Εγκατάσταση UPS/γεννήτριας	Έγκριση σχετικού κονδυλίου	Διαχειριστής Συστημάτων και Δικτύου	Κάθε 6 μήνες
11	Απολύσεις προσωπικού χωρίς να εφαρμοστεί η σχετική διαδικασία ασφαλείας	0	Πολιτική τερματισμού απασχόλησης προσωπικού	-	Διευθυντής Ανθρώπινου Δυναμικού	Κάθε 6 μήνες
12	Έλεγχος ασφαλείας σε όλες τις εφαρμογές mobile agents	100% συμμόρφωση	Διαδικασία ελέγχου ασφαλείας εφαρμογών	Απομονωμένο δίκτυο υπολογιστών και λογισμικό ελέγχου ασφάλειας	Προγραμματιστές	Κάθε 6 μήνες
13	Αριθμός Ευπαθειών Συστημάτων & Δικτύου	<=3	Penetration Testing	Διαθεσιμότητα του εμπλεκόμενου προσωπικού για μισή εργάσιμη ημέρα.	Διευθυντής Ασφάλειας Πληροφοριών / Εσωτερικός Ελεγκτής	Κάθε 6 μήνες

14	Ανασκόπηση αξιολόγησης/αντιμετώπισης κινδύνου	100% συμμόρφωση	Διαδικασία αξιολόγησης/αντιμετώπισης κινδύνου	Διαθεσιμότητα του εμπλεκόμενου προσωπικού.	Διευθυντής Ασφάλειας Πληροφοριών	Κάθε 6 μήνες

Πίνακας 3.5: Οι στόχοι ασφάλειας πληροφοριών

3.2.10 Πόροι (Παράγραφος 7.1)

Ο οργανισμός πρέπει να καθορίσει και να αποδεσμεύσει τους αναγκαίους πόρους για την εγκαθίδρυση, υλοποίηση, συντήρηση και συνεχή βελτίωση του ΣΔΑΠ. Αυτοί οι πόροι μπορεί να είναι: χρήματα, αγορά νέου ή αναβάθμιση εξοπλισμού, κατάλληλες εγκαταστάσεις, πρόσληψη εξειδικευμένου προσωπικού, κ.τ.λ.

3.2.11 Επαγγελματική επάρκεια (Παράγραφος 7.2)

Το προσωπικό που εργάζεται στον οργανισμό πρέπει να έχει την κατάλληλη επαγγελματική επάρκεια και γνώση σε θέματα που αφορούν τα καθήκοντα τους όπως επίσης και την ασφάλεια των πληροφοριών του οργανισμού. Σε αυτή την παράγραφο, υπάρχουν οι απαιτήσεις για τον καθορισμό και την διασφάλιση της επαγγελματικής επάρκειας του προσωπικού κατά την πρόσληψη, ενώ όταν προκύψει η ανάγκη ο οργανισμός πρέπει να φροντίσει ώστε το προσωπικό να εκπαιδευτεί κατάλληλα (π.χ. με παρακολούθηση σεμιναρίων). Τέλος, ο οργανισμός πρέπει να διατηρεί αρχείο ως απόδειξη της επαγγελματικής επάρκειας.

3.2.12 Ευαισθητοποίηση (Παράγραφος 7.3)

Όλο το προσωπικό του οργανισμού πρέπει να είναι ενήμερο για τις πολιτικές ασφάλειας του οργανισμού, την συνεισφοράς του στο ΣΔΑΠ και τα πλεονεκτήματα της εφαρμογής του, αλλά και για τις επιπτώσεις της μη συμμόρφωσης με τις απαιτήσεις του ΣΔΑΠ.

3.2.13 Επικοινωνία (Παράγραφος 7.4)

Η επικοινωνία των ενδιαφερόμενων μερών είναι ένα πολύ σημαντικό κομμάτι του ΣΔΑΠ, είτε αυτή είναι εσωτερική (εντός του οργανισμού) είτε εξωτερική (π.χ. με τους εξωτερικούς συνεργάτες). Ο οργανισμός πρέπει να καθορίσει:

- Το άτομο που θα είναι υπεύθυνο για την επικοινωνία.
- Το περιεχόμενο της επικοινωνίας.
- Πότε θα πραγματοποιηθεί η επικοινωνία.
- Πού θα πραγματοποιηθεί η επικοινωνία (το κανάλι επικοινωνίας).
- Τα άτομα που θα συμμετέχουν στην επικοινωνία.
- Τις διαδικασίες με τις οποίες θα πραγματοποιηθεί η επικοινωνία.

Το περιεχόμενο της επικοινωνίας μπορεί να είναι:

- Οι πολιτικές ασφαλείας και οι διαδικασίες ή οι ενημερωμένες εκδόσεις τους.
- Νομοθεσία (π.χ. Εφαρμογή του GDPR)
- Γνώση σχετικά με νέες απειλές και τρόπους αντιμετώπισης τους.
- Οι στόχοι ασφαλείας.
- Περιπτώσεις έκτακτης ανάγκης (π.χ. άσκηση ετοιμότητας).
- Ενημέρωση για εκπαίδευση/εκδηλώσεις σχετικές με την ασφάλεια πληροφοριών.
- Αλλαγές που έγιναν στο ΣΔΑΠ.

Ο καθορισμός της επικοινωνίας γίνεται στο Αρχείο Καταγραφής 008 και δίνεται στο **Παράρτημα Δ**.

3.2.14 Τεκμηριωμένες Πληροφορίες (Παράγραφος 7.5)

Το ΣΔΑΠ του οργανισμού δεν πρέπει να συμπεριλαμβάνει μόνο τις τεκμηριωμένες πληροφορίες που απαιτεί το πρότυπο ISO 27001:2013 αλλά και αυτές τις πληροφορίες που είναι αναγκαίες για την σωστή και αποτελεσματική λειτουργία του.
Τις απαιτήσεις του προτύπου όπως: αναγνωριστικά εγγράφων, κοινή μορφοποίηση, έγκριση από την διοίκηση , έλεγχος αλλαγών, κ.α. τις εφαρμόσαμε στα έγγραφα που δημιουργήσαμε για τον οργανισμό-μοντέλο **Παραρτήματα Α, Β, Γ, Δ, Ε, Ζ, Η**.

3.2.15 Σχεδιασμός, λειτουργία και έλεγχος των διεργασιών (Παράγραφος 8)

Ο οργανισμός πρέπει να σχεδιάσει, υλοποιήσει, ελέγξει και τεκμηριώσει τις διαδικασίες που χρειάζεται ώστε να συμμορφώνεται με τις απαιτήσεις ασφαλείας, αλλά και να υλοποιεί τις ενέργειες για την αντιμετώπιση των κινδύνων και της αξιοποίησης των ευκαιριών ώστε να πετύχει τους στόχους που έθεσε.

Ο οργανισμός πρέπει να διενεργεί και να τεκμηριώνει την διαδικασία της διαχείρισης κινδύνων (αξιολόγηση και αντιμετώπιση) ανά τακτά χρονικά διαστήματα ή κάθε φορά που γίνονται σημαντικές αλλαγές (π.χ. ενσωμάτωση ενός νέου συστήματος ή υπηρεσίας στο δίκτυο του οργανισμού). Στην περίπτωση του οργανισμού-μοντέλου που δημιουργήσαμε η τεκμηρίωση της διαδικασίας έγινε στην διαδικασία 006.

3.2.16 Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση (Παράγραφος 9.1)

Οι επιδόσεις της ασφάλειας των πληροφοριών αλλά και του ίδιου του ΣΔΑΠ πρέπει να παρακολουθούνται, να γίνεται η μέτρηση τους, να αναλύονται και να αξιολογούνται. Ο οργανισμός πρέπει να διατηρεί κατάλληλες τεκμηριωμένες πληροφορίες ως αποδεικτικό στοιχείο της παρακολούθησης και της μέτρησης.

Στην περίπτωση του οργανισμού-μοντέλου που δημιουργήσαμε, κάναμε την σχετική τεκμηρίωση στην πολιτική 014 (απαιτήσεις ελέγχων επιθεώρησης υπολογιστικών συστημάτων) αλλά και στην διαδικασία 010 (εσωτερική επιθεώρηση).

3.2.17 Εσωτερική επιθεώρηση (Παράγραφος 9.2)

Ο οργανισμός πρέπει να διενεργεί εσωτερικές επιθεωρήσεις του ΣΔΑΠ ανά τακτά χρονικά διαστήματα, ούτος ώστε να λαμβάνει πληροφορίες σχετικά με την αποτελεσματικότητα και την συμμόρφωσή με τις απαιτήσεις του, αλλά και με τις απαιτήσεις του πρότυπου ISO 27001:2013.

Στην περίπτωση του οργανισμού-μοντέλου που δημιουργήσαμε η διαδικασία της εσωτερικής επιθεώρησης περιγράφεται στην διαδικασία 010, ενώ δημιουργήσαμε και σχετική φόρμα αναφοράς (Φόρμα 002).

3.2.18 Ανασκόπηση διοίκησης (Παράγραφος 9.3)

Η διοίκηση του οργανισμού, πρέπει να διενεργεί ανασκόπηση του ΣΔΑΠ ανά τακτά χρονικά διαστήματα ούτος ώστε να διασφαλίζει την συνεχή επάρκεια, καταλληλόλητα και την αποτελεσματικότητα του. Η ανασκόπηση της διοίκησης πρέπει να είναι τεκμηριωμένη πληροφορία και επιπλέον να περιλαμβάνει τις αποφάσεις που είναι σχετικές με την συνεχή βελτίωση του ΣΔΑΠ.

Στην περίπτωση του οργανισμού-μοντέλου, δημιουργήσαμε μια σχετική φόρμα αναφοράς της ανασκόπησης από την διοίκηση (Φόρμα 003).

3.2.19 Μη συμμόρφωση και διορθωτικές ενέργειες (Παράγραφος 10.1)

Οι μη συμμορφώσεις με τις απαιτήσεις του ΣΔΑΠ, μπορεί να διαπιστωθούν κατά τη διαδικασία της εσωτερικής επιθεώρησης, κατά την διάρκεια τυχαίων δειγματοληπτικών ελέγχων ή μετά από την αναφορά ενός γεγονότος ή περιστατικού από το προσωπικό.

Στην περίπτωση του οργανισμού-μοντέλου, δημιουργήσαμε οι ενέργειες που πρέπει να ακολουθήσει ο οργανισμός περιγράφονται στην πολιτική 018 και διαδικασίες 009 και 010.

3.2.20 Συνεχής βελτίωση (Παράγραφος 10.2)

Στην τελευταία παράγραφο το πρότυπο ISO 27001, απαιτεί από τον οργανισμό να βελτιώνει διαρκώς το ΣΔΑΠ ώστε να διασφαλίσει την συνεχή επάρκεια, καταλληλόλητα και την αποτελεσματικότητα του.

Κεφάλαιο 4
Μελέτη Περιπτώσεων

4.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα προσπαθήσουμε να απαντήσουμε τα ερευνητικά ερωτήματα που θέσαμε στο Κεφάλαιο 1, μελετώντας κάποια ρεαλιστικά σενάρια περιπτώσεων από τις απαιτήσεις του ΣΔΑΠ του οργανισμού-μοντέλου που υλοποιήσαμε στο Κεφάλαιο 3. Όλες οι περιπτώσεις έχουν άμεση σχέση με την ασφάλεια των mobile agents. Άλλες απαιτήσεις, πολιτικές ή διαδικασίες που υλοποιήσαμε στο κεφάλαιο 3 και δεν θα τις δούμε σε αυτό το κεφάλαιο, προσφέρουν και αυτές με τον τρόπο τους ασφάλεια στους mobile agents, αλλά έμμεσα.
Στην δημιουργία αυτών των σεναρίων βοήθησε σε μεγάλο βαθμό η εκπαίδευσή η εμπειρία του ερευνητή, αλλά και οι θεματικές ενότητες του προγράμματος μεταπτυχιακών σπουδών «Ασφάλεια Υπολογιστών και Δικτύων» του Ανοικτού Πανεπιστημίου Κύπρου.

Ο λόγος που επιλέξαμε αυτή την ερευνητική στρατηγική είναι γιατί μας δίνει την δυνατότητα να απαντήσουμε ερευνητικά ερωτήματα τύπου «πώς;» και «γιατί;» σε εμπειρικά γεγονότα που δεν έχουμε τον πλήρη έλεγχο [42]. Τους περιορισμούς αυτούς τους εξηγούμε αναλυτικότερα στο επόμενο κεφάλαιο.

Στις μελέτες περίπτωσης 3 και 4, κάναμε κάποιες δοκιμές σε περιβάλλον mobile agents, χρησιμοποιώντας την πλατφόρμα Aglets έκδοση 2.5 και το Aglets Software Development Kit (ASDK). Για την μελέτη αυτών των περιπτώσεων, δημιουργήσαμε και εφαρμόσαμε μια διαδικασία με τον κύκλο ζωής του λογισμικού (Διαδικασία 008), που βασίζεται στην μεθοδολογία Plan-Do-Check-Act που προωθεί το ISO 27001 σε συνδυασμό με τις φάσεις του SDLC (Software Development Life Cycle)[34].

4.2 Μελέτη περίπτωσης 1: Ασφάλεια Πλατφόρμας Mobile Agent

Ο διευθυντής ασφάλειας πληροφοριών του οργανισμού XYZ, μετά από ενημέρωση που είχε από ένα έγκυρο τεχνολογικό blog που εξειδικεύεται στην ασφάλεια υπολογιστών και δικτύων, μαθαίνει για ένα νέο κενό ασφαλείας που επηρεάζει τα Java Keystores τύπου JKS (η default επιλογή).

Το κενό ασφαλείας είχε να κάνει με την παράκαμψη του κωδικού του keystore και την έκθεση της τιμής κατακερματισμού (hashes) των ιδιωτικών κλειδιών κάνοντας το έτσι ευάλωτο σε επιθέσεις λεξικού (dictionary attack) αλλά και επιθέσεις εξαντλητικών δοκιμών (brute force attack). KeyStores χρησιμοποιεί και η πλατφόρμα Aglets για την αποθήκευση των κλειδιών για την αυθεντικοποίηση των χρηστών.

Θέλοντας να δοκιμάσει την ασφάλεια των keystore της πλατφόρμας Aglets, αλλά και να διαπιστώσει κατά πόσο ο οργανισμός είναι εκτεθειμένος στο κενό ασφαλείας, προχώρησε σε αντιγραφή ενός keystore και προσπάθησε να αποσπάσει τα hashes σύμφωνα με τις οδηγίες του άρθρου (πολιτική 018). Ακολουθούν τα βήματα που ακολούθησε:

Βήμα 1: Έκθεση τιμών κατακερματισμού με το εργαλείο JksPrivkPrepare.jar [26]

```
> java -jar JksPrivkPrepare.jar .keystore > hash.txt
Alias: anonymous, algorithm: DSA, keysize or field size: 1024
Alias: aglet_key, algorithm: DSA, keysize or field size: 1024
```

Εικόνα 4.1: Χρήση του εργαλείου JksPrivkPrepare.

Έξοδος:

hash.txt

```
1  $jksprivk$*2DB665D548964611181A1F47F0D1D859C01C007BB*0B4A1BA5FC5CD2B851846AC2428131E370AADA11*426E53E077E38AE2
   469D3F0D545ED1B919D22155E9846199B55014870B99B0FEE359B2199F6274B5B7BADA68038CBE5A72E8679DCE7B74996F51B69A5469F
   C998E22ACEDA0F4F05E5313CF3E862615B343857D8CFFA5C8908E65FADA6D6B98013F55485E094122D9312440D7036EC1816E9AB70574
   6F4C6D99F40197CD82749C01DB9E9BE302A7AD993623D6F41E8B1C9B7047F2E4BF7BC3612094F029F4D941C2D7CE55DFAF1EE1DAB6F71
   48BC4BFDCFB4E145D74DA7F4EE49F156503CD22D85773152B456D024F72557380E25043184CB8AA85ADF63BD25A556F9B4015018413D9
   67F63D9F7BD05373A0EF8E731F046A13955088D98C200BD69DE31425AFB383F0A355AA83640472A0991E91896FF404CFA26DC1B93BCBB
   F65FD1AAF7DAAB045B4BEA5CBC794491237B1977788877E5FD663B357C9D4D15B0E117B30AC02D02B9797B599E7F215537E5FC90521D0
   *72*8AD2C49C130B537457F1D7EA2554*anonymous
2  $jksprivk$*E2C900B18ED7C3503F8FCFCB3E43B3FA3D1EF2F0*E99A791B880014A7C1120B075028D163F9BC237F*AE5075D98C7F849B
   47F8B637ABD3F5AF998DC7EAC32C636D7E1DF75B7E18FFB3B541188DE09F160EAE8D5B0516FE60D0AFE3ABE7371E7DDF181EC43556FDC
   D3AB24825B5185B440E093B9885F726DDC0550684ED2C143B6FEAC6405475EDF9ABF4703F3877D43D12146D0DA715A7D75F4BC9FFD02E
   A365A29A25AAE46D3EA144E47B171E5DD785E721853F35FC0442837BBACAB9F9CABC0B3A6CF4CC93E31A51BB863B1F98FE411C4730D02
   5BC1E5527D666A2C6DD0E4807A79C150BD8946BC5B2C7A6B9F071F4C9015FFD26354C09B3176D7C882F22613D7462194318B00268F1EF
   C7E689D3F5A62C28E49896490217F3B7BB80A9D9D81C49BE6C4168FDCE01956C4F30F141B4E94A8F960A95EDA8D0CD487D754E24BA707
   D45FAAB60516234C0FB243FB1035473D3BCA79FF30506855067C62149BC89B150BA0B892798F1BA4D7D3094908F8905EBBB82FDDC9B36
   *9E*84ABC5F99A31ACF973E757B5C3EB*aglet_key
```

Εικόνα 4.2: Οι τιμές κατακερματισμού (hashes) των χρηστών της πλατφόρμας Aglets, οι οποίες έχουν αποκαλυφθεί με την χρήση του εργαλείου JksPrivkPrepare.

Σε αυτό το σημείο ο διευθυντής ασφάλειας πληροφοριών διαπιστώνει ότι τα ιδιωτικά κλειδιά για την πρόσβαση στην πλατφόρμα Aglets είναι ευάλωτα. Ένας σοβαρός κίνδυνος που υπάρχει είναι η είσοδος στην πλατφόρμα από μη εξουσιοδοτημένα άτομα και αποστολή κακόβουλων mobile agents προς εκτέλεση.

Αμέσως, επικοινωνεί με την υποστήριξη πελατών της πλατφόρμας Aglets για άμεση λήψη διορθωτικών ενεργειών και κλείσιμο του κενού ασφαλείας. Σύμφωνα με την συμφωνία επιπέδου υπηρεσίας (SLA) που έχει υπογραφή από τα δυο μέρη, τα περιστατικά ασφαλείας πρέπει να αντιμετωπίζονται εντός 48 ωρών (Πολιτική 015, Διαδικασία 009). Όπως και έγινε. Ο πάροχος της πλατφόρμας Aglets την επόμενη μέρα, υλοποίησε μια ενημέρωση ασφαλείας κάνοντας αλλαγή του τύπου keystore σε JCEKS που παρέχει μεγαλύτερη ασφάλεια.

Ο διευθυντής ασφάλειας πληροφοριών θέλοντας να προχωρήσει ένα βήμα παρακάτω προσπάθησε να αποσπάσει τα ιδιωτικά κλειδιά με την χρήση της εφαρμογής hashcat [27] και την χρήση μιας λίστας πιθανόν κωδικών (dictionary). Το hashcat είναι μια εφαρμογή που μπορεί να αποκαλύψει κωδικούς πρόσβασης γνωρίζοντας τις τιμές κατακερματισμού (hashes). Μεταξύ άλλων, η εφαρμογή, υποστηρίζει και τις τιμές κατακερματισμού των ιδιωτικών κλειδιών των keystores τύπου JKS (SHA1).

Βήμα 2: Απόπειρα απόσπασης του ιδιωτικού κλειδιού με την εφαρμογή hashcat

Μετά από την εκτέλεση της εφαρμογής hashcat (Εικόνες 4.3 και 4.4) διαπιστώνει με έκπληξη του ότι όχι μόνο ο κωδικός (‘aglets’) έχει αποκαλυφθεί πολύ ευκολά, αλλά και ότι δεν έχει αλλάξει αμέσως μετά από την εγκατάσταση της πλατφόρμας στους servers παραγωγής. Πρόκειται για τον default κωδικό χρήστη.

```
hashcat64.exe -m 15500 -a 0 ..\hash.txt ..\wordlist.txt --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: Intel(R) Corporation
========================================
* Device #1: Intel(R) HD Graphics 4400, 407/1629 MB allocatable, 20MCU
* Device #2: Intel(R) Core(TM) i3-4005U CPU @ 1.70GHz, skipped.

Hashes: 2 digests; 2 unique digests, 2 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Not-Iterated

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Dictionary cache hit:
* Filename..: ..\wordlist.txt
* Passwords.: 2
* Bytes.....: 19
* Keyspace..: 2

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.
```

Εικόνα 4.3: Επίθεση λεξικού με την εφαρμογή hashcat

```
$jksprivk$*E2C900B18ED7C3503F8FCFCB3E43B3FA3D1EF2F0*E99A791B880014A7C1120B075028D163
F9BC237F*AE5075D98C7F849B47F8B637ABD3F5AF998DC7EAC32C636D7E1DF75B7E18FFB3B541188DE09
F160EAE8D5B0516FE60D0AFE3ABE7371E7DDF181EC43556FDCD3AB24825B5185B440E093B9885F726DDC
0550684ED2C143B6FEAC6405475EDF9ABF4703F3877D43D12146D0DA715A7D75F4BC9FFD02EA365A29A2
5AAE46D3EA144E47B171E5DD785E721853F35FC0442837BBACAB9F9CABC0B3A6CF4CC93E31A51BB863B1
F98FE411C4730D025BC1E5527D666A2C6DD0E4807A79C150BD8946BC5B2C7A6B9F071F4C9015FFD26354
C09B3176D7C882F22613D7462194318B00268F1EFC7E689D3F5A62C28E49896490217F3B7BB80A9D9D81
C49BE6C4168FDCE01956C4F30F141B4E94A8F960A95EDA8D0CD487D754E24BA707D45FAAB60516234C0F
B243FB1035473D3BCA79FF30506855067C62149BC89B150BA0B892798F1BA4D7D3094908F8905EBBB82F
DDC9B36*9E*84ABC5F99A31ACF973E757B5C3EB*aglet_key:aglets
$jksprivk$*2DB665D54896461118A1F47F0D1D859C01C007BB*0B4A1BA5FC5CD2B851846AC2428131E3
70AADA11*426E53E077E38AE2469D3F0D545ED1B919D22155E9846199B55014870B99B0FEE359B2199F6
274B5B7BADA68038CBE5A72E8679DCE7B74996F51B69A5469FC998E22ACEDA0F4F05E5313CF3E862615B
343857D8CFFA5C8908E65FADA6D6B98013F55485E094122D9312440D7036EC1816E9AB705746F4C6D99F
40197CD82749C01DB9E9BE302A7AD993623D6F41E8B1C9B7047F2E4BF7BC3612094F029F4D941C2D7CE5
5DFAF1EE1DAB6F7148BC4BFDCFB4E145D74DA7F4EE49F156503CD22D85773152B456D024F72557380E25
043184CB8AA85ADF63BD25A556F9B4015018413D967F63D9F7BD05373A0EF8E731F046A13955088D98C2
00BD69DE31425AFB383F0A355AA83640472A0991E91896FF404CFA26DC1B93BCBBF65FD1AAF7DAAB045B
4BEA5CBC794491237B1977788877E5FD663B357C9D4D15B0E117B30AC02D02B9797B599E7F215537E5FC
90521D0*72*8AD2C49C130B537457F1D7EA2554*anonymous:aglets

Session..........: hashcat
Status...........: Cracked
Hash.Type........: JKS Java Key Store Private Keys (SHA1)
Hash.Target......: ..\hash.txt
Time.Started.....: Mon Mar 25 19:02:54 2019 (0 secs)
Time.Estimated...: Mon Mar 25 19:02:54 2019 (0 secs)
Guess.Base.......: File (..\wordlist.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      429 H/s (0.06ms) @ Accel:64 Loops:1 Thr:64 Vec:1
Recovered........: 2/2 (100.00%) Digests, 2/2 (100.00%) Salts
Progress.........: 4/4 (100.00%)
Rejected.........: 0/4 (0.00%)
Restore.Point....: 0/2 (0.00%)
Restore.Sub.#1...: Salt:1 Amplifier:0-1 Iteration:0-1
Candidates.#1....: aglets -> anonymous

Started: Mon Mar 25 19:02:52 2019
Stopped: Mon Mar 25 19:02:55 2019
```

Εικόνα 4.4: Η αποκάλυψη των κωδικών των χρηστών

Βήμα 3: Οι επόμενες Ενέργειες:

Οι επόμενες ενέργειες που ακολούθησε ο διευθυντής ασφάλειας πληροφοριών ήταν:

1. Άμεση αλλαγή του κωδικού της πλατφόρμας βάση της πολιτικής 009 από τον υπεύθυνο της πλατφόρμας (Πολιτική 009: Σύστημα Διαχείρισης Κωδικών Πρόσβασης).
2. Ενημέρωση του αρχείου καταγραφής 009 ως γεγονός (event).
3. Ενημέρωση του αρχείου καταγραφής 009 με τις διορθωτικές ενέργειες που ελήφθησαν.
4. Λήψη πειθαρχικών μέτρων για μεγάλα παραπτώματα (Διαδικασία 002) και αποστολή γραπτής προειδοποίησης στον υπεύθυνο της πλατφόρμας Aglets (Προγραμματιστής). Ο λόγος ήταν η μη τήρηση της πολιτικής 009 του οργανισμού.
5. Ενημέρωση της πολιτικής 010 (Χρήση Κρυπτογράφησης) για χρήση keystores τύπου JCEKS σε εφαρμογές που αναπτύσσει ο οργανισμός, βελτιώνοντας με αυτό τον τρόπο το ΣΔΑΠ (Παράγραφος 10.2 του ISO 27001:2013).
6. Αποστολή της ενημερωμένης πολιτικής στο προσωπικό και ενημέρωση του αρχείου καταγραφής 008.

4.3 Μελέτη περίπτωσης 2: Ασφάλεια Mobile Agents σε οργανωτικό επίπεδο

Ο κύριος λόγος που ο οργανισμός XYZ προχώρησε στην υλοποίηση ενός ΣΔΑΠ με βάση τις απαιτήσεις του διεθνούς προτύπου ISO 27001:2013, ήταν ένα περιστατικό όπου ένας προγραμματιστής αφού «έκλεψε» την καινοτόμα ιδέα ενός mobile agent (τον σχεδιασμό και μέρος του πηγαίου κώδικα) που ανέπτυξε ο οργανισμός, παραιτήθηκε από τον οργανισμό δυόμιση μήνες πριν την διάθεση του στην αγορά.

Δυο εβδομάδες μετά ο συγκεκριμένος υπάλληλος ξεκίνησε να εργάζεται ως διευθυντής του τμήματος ανάπτυξης λογισμικού σε ανταγωνιστική εταιρία, που εργοδοτούσε τον τριπλάσιο αριθμό προγραμματιστών και πέντε εβδομάδες μετά, η ανταγωνιστική εταιρία διάθεσε στην αγορά την εφαρμογή mobile agent, λίγες μέρες δηλαδή πριν την προγραμματισμένη διάθεση της από τον οργανισμό XYZ. Οι διαφορές με την εφαρμογή που ανέπτυσσε ο οργανισμός XYZ ήταν ελάχιστες.

Σημειώνεται ότι εκείνο το διάστημα στον οργανισμό XYZ ίσχυαν τα παρακάτω:

- Δεν υπήρχαν υλοποιημένες πολιτικές και διαδικασίες ασφάλειας.
- Δεν υπήρχε σήμανση ότι απαγορεύεται η φωτογράφηση/βιντεοσκόπηση εντός των κτιριακών εγκαταστάσεων του οργανισμού.
- Δεν γινόταν διαχείριση (αξιολόγηση και αντιμετώπιση) των κινδύνων
- Δεν υπήρχε υπογεγραμμένο σύμφωνο εμπιστευτικότητας με το προσωπικό.
- Υπήρχε συμβόλαιο εργοδότησης αλλά δεν γινόταν αναφορά στην ασφάλεια των περιουσιακών στοιχείων του οργανισμού.
- Υπήρχε κλειστό κύκλωμα τηλεόρασης αλλά μόνο περιμετρικά των κτιριακών εγκαταστάσεων και όχι μέσα στα γραφεία.
- Ο σχεδιασμός της εφαρμογής γινόταν πάνω σε πίνακες που υπήρχαν στα γραφεία του τμήματος, δεν τεκμηριωνόταν ο σχεδιασμός με άλλο τρόπο. Ο κάθε προγραμματιστής κρατούσε σημειώσεις.

Αν και υπήρξαν μαρτυρίες από συναδέλφους του προγραμματιστή ότι συχνά κρατούσε προσωπικές γραπτές σημειώσεις και ότι έβγαζε φωτογραφίες με το κινητό του, δεν υπήρχαν αρκετά αποδεικτικά στοιχεία εναντίον του για να στοιχειοθετηθεί υπόθεση και να κινηθούν νομικά εναντίον του. Επιπλέον δεν υπήρχαν οι σχετικές πολιτικές που να απαγορεύουν τη λήψη φωτογραφιών και την τήρηση προσωπικών σημειώσεων και μεταφορά τους εκτός του οργανισμού.

Μετά από αυτό το περιστατικό, ο οργανισμός αποφάσισε να εφαρμόσει ένα ΣΔΑΠ, υλοποιώντας μεταξύ άλλων τα παρακάτω, με σκοπό να μην επαναληφθούν ανάλογα ή χειρότερα περιστατικά στο μέλλον μιας και οι οικονομικές επιπτώσεις ήταν τεράστιες:

- Υλοποίηση διαδικασίας διαχείρισης κινδύνων (Διαδικασία 006)
- Υλοποίηση Σχεδιασμού για φυσική και περιβαλλοντική ασφάλειας με επιπλέον κάμερες ασφάλειας εντός των γραφείων και απαγόρευση της λήψης φωτογραφιών (Σχεδιασμός 002).
- Υπογραφή συμφώνου εμπιστευτικότητας με όλο το προσωπικό αλλά και τους εξωτερικούς συνεργάτες (NDA 001).
- Ενημέρωση της σύμβαση εργασίας αορίστου χρόνου (Συμβόλαιο 001) με τις παραγράφους 4 και 6 που δίνεται η συγκατάθεση καταγραφής από το σύστημα CCTV και απαγορεύουν την τήρηση προσωπικών σημειώσεων.
- Υλοποίηση διαδικασίας αναφοράς περιστατικού ασφαλείας από το προσωπικό (Διαδικασία 009).
- Υλοποίηση πειθαρχικής διαδικασίας (Διαδικασία 002). Παρόμοια παραπτώματα θα αντιμετωπίζονται ως «Πολύ σοβαρά παραπτώματα».
- Υλοποίηση πολιτικής καθαρού γραφείου/καθαρής οθόνης (Πολιτική 011)
- Υλοποίηση πολιτικής και διαδικασίας που αφορούν την ασφαλή ανάπτυξη λογισμικού (Πολιτική 016, Διαδικασία 008).

4.4 Μελέτη περίπτωσης 3: Ασφάλεια Mobile Agents - Δοκιμή RSA με δυο Hosts

Σε αυτή την μελέτη περίπτωσης θα μελετήσουμε την ασφαλή μεταφορά δεδομένων μεταξύ δυο host, με την χρήση ενός mobile agent στη πλατφόρμα Aglets και τον αλγόριθμο κρυπτογράφησης RSA. Η χρήση κρυπτογραφίας γίνεται για την διασφάλιση της εμπιστευτικότητας και της ακεραιότητας κατά την μετάδοση των ευαίσθητων δεδομένων από την εφαρμογή. Στην Εικόνα 4.5 βλέπουμε την τοπολογία δικτιού που θα χρησιμοποιήσουμε για την δοκιμή μας.

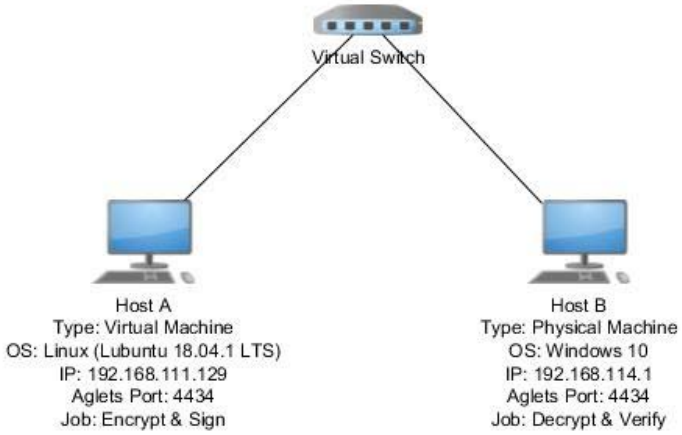
Η διαδικασία είναι σχετικά απλή. Στον Host A θα γίνεται η δημιουργία, η κρυπτογράφηση και η υπογραφή των δεδομένων ενώ στον Host B θα γίνεται η αποκρυπτογράφηση και η επαλήθευση των δεδομένων. Ο ρόλος του mobile agent είναι να μεταφέρει τα κρυπτογραφημένα δεδομένα από τον Host A στον Host B, ενώ δεν εμπλέκεται καθόλου στην διαδικασία κρυπτογράφησης – αποκρυπτογράφησης [8, 22, 23, 24, 25].

Στους δυο Hosts δίνονται τα σχετικά δικαιώματα σε συγκεκριμένους πόρους των συστημάτων, συγκεκριμένα:

- Δικαίωμα εγγραφής και ανάγνωσης αρχείων (File Permissions)
- Δικαίωμα αποδέσμευσης και μεταφοράς (dispatch) του mobile agent.

Τέλος, υλοποιήσαμε ένα σύστημα καταγραφής συμβάντων (Log File) που έχει σκοπό την παρακολούθηση και ανάλυση της συμπεριφοράς του mobile agent.

Ο πηγαίος κώδικας (Java) δίνεται στο **Παράρτημα Θ (Θ.1, Θ.2 και Θ.3)**.



Εικόνα 4.5: Η τοπολογία του δικτύου δοκιμής

Ακολουθούν αναλυτικά τα βήματα:

Βήμα 1: Δημιουργία ζεύγους ιδιωτικού - δημοσίου κλειδιού (σε KeyStores) για τον κάθε Host

- Για τον Host A (HostSoftware -> Host_A_Writer):

```
keytool -genkeypair -alias host_a -storepass 123456a -keypass a65432
1 -keyalg RSA -keystore keystore_of_host_A.jceks -storetype jceks
```

- Για τον Host B (HostSoftware -> Host_B_Reader):

```
keytool -genkeypair -alias host_b -storepass 123456b -keypass b654321 -keyalg
RSA -keystore keystore_of_host_B.jceks -storetype jceks
```

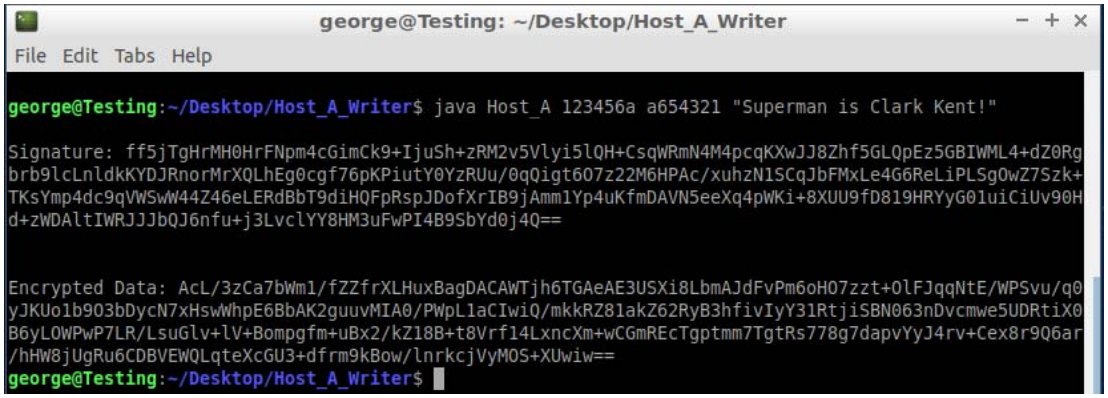
Βήμα 2: Εξαγωγή πιστοποιητικών (export) και ανταλλαγή δημόσιων κλειδιών (import)

- Για τον Host A (αποθήκευση στο HostSoftware -> Host_B_Reader):
    - `keytool -export -keystore keystore_of_host_A.jceks -alias host_a -file host_a_pub.cer -storetype jceks`
    - `keytool -import -alias host_b -file host_b_pub.cer -keystore keystore_of_host_A.jceks -storetype jceks`

- Για τον Host B (αποθήκευση στο HostSoftware -> Host_A_Writer)::
    - `keytool -export -keystore keystore_of_host_B.jceks -alias host_b -file host_b_pub.cer -storetype jceks`
    - `keytool -import -alias host_a -file host_a_pub.cer -keystore keystore_of_host_B.jceks -storetype jceks`

Βήμα 3: Υπογραφή με το ιδιωτικό κλειδί του Α και κρυπτογράφηση με το δημόσιο κλειδί του Β

- Εκτέλεση στον Host A της εφαρμογής Host_A.java
- Δημιουργία αρχείων data_sig.txt (υπογραφή) και enc_data.txt (κρυπτογραφημένα δεδομένα)



Εικόνα 4.6: Η εκτέλεση στον Host A

Βήμα 4: Καθορισμός Πολιτικής Ασφάλειας Agent στον Host A

Αρχείο: aglets.policy (<aglets directory>/.aglets/security)

```
grant
codeBase "file:/C:/aglets/public/MSc"
{
permission java.io.FilePermission "/home/george/Desktop/Host_A_Writer/enc_data.txt",
"read";
permission java.io.FilePermission "/home/george/Desktop/Host_A_Writer/data_sig.txt",
"read";
permission com.ibm.aglets.security.AgletPermission "george", "dispatch";
};
```

Βήμα 5: Καθορισμός Πολιτικής Ασφάλειας Agent στον Host B

Αρχείο: aglets.policy (<aglets directory>/.aglets/security)

```
grant
codeBase "file:/C:/aglets/public/MSc"
{
    permission java.io.FilePermission "C:\\Host_B_Reader\\enc_data.txt", "write";
    permission java.io.FilePermission "C:\\Host_B_Reader\\data_sig.txt", "write";
    permission java.io.FilePermission "C:\\Host_B_Reader\\Log.txt", "write";
    permission com.ibm.aglets.security.AgletPermission "george", "dispatch";
};
```

Βήμα 6: Εκτέλεση του Mobile Agent στον Host B

Αρχείο: mytest.java

Η «αποστολή» του agent είναι το διάβασμα και μεταφορά/αντιγραφή των δεδομένων data_sig.txt (ψηφιακή υπογραφή) και enc_data.txt (κρυπτογραφημένα δεδομένα) από τον Host A στον Host B.

Ο mobile agent «φεύγει» από τον Host B διαβάζει τα παραπάνω δεδομένα από τον Host A και στην συνέχεια επιστρέφει ξανά στον Host B. Δεν εμπλέκεται στην διαδικασία κρυπτογράφησης / αποκρυπτογράφησης.

Στον Host A:

```
INFO - Authenticated user george
[Warning: The hostname seems not having domain name.
 Please try -resolve option to resolve the fully qualified hostname
 or use -domain option to manually specify the domain name.]
INFO - USE SECURE RANDOM SEED.
INFO - AUTHENTICATION MODE OFF.
INFO - AgletThreadPool starting with 10 min threads
INFO - AgletThreadPool ready
INFO - Creating ResourceManager.
My Test Arrived!

Done! Bye Bye!


***** Addr: atp://192.168.114.1 place:
No integrity check because no security domain is authenticated.
```

Εικόνα 4.7: Η εκτέλεση του mobile agent στον Host A

Στον Host B:

```
INFO - Classpath is specified as lib;lib\classes;lib\aglets-2.5-gamma.jar;lib\log4j-1.2.16.jar;;.\public
INFO - Real classpath = lib;lib\classes;lib\aglets-2.5-gamma.jar;lib\log4j-1.2.16.jar;
INFO - Logging system initialized!
INFO - Reading security policy file: C:\Program Files\Java\jre1.8.0_201\lib\security\java.policy
INFO - Reading security policy file: C:\aglets\.aglets\security\aglets.policy
INFO - Loading shared secrets from file C:\aglets\.aglets\security\secrets.dat
INFO - No shared secret file.
INFO - No secrets.
[Warning: The hostname seems not having domain name.
 Please try -resolve option to resolve the fully qualified hostname
 or use -domain option to manually specify the domain name.]
INFO - USE SECURE RANDOM SEED.
INFO - AUTHENTICATION MODE OFF.
INFO - AgletThreadPool starting with 10 min threads
INFO - AgletThreadPool ready
INFO - Creating ResourceManager.
My Test Created
***** Addr: atp://192.168.111.129 place:
No integrity check because no security domain is authenticated.
INFO - Creating ResourceManager.
My Test Arrived!

Encrypted Data: d+nbcg/z6h+Ij9bixbjK7OQqW9emXmAcI2lJRTr1y6jumBku4DHXVa45K86WO7zvXG6giQ4t2K0tbvoLp6zrLjFkGEtp9nP1fLqq6bkS
8mzsymfu3gXF5nZ9N69/CT1h7QMetNrLlVkbnl5gmEV93/tvFlH633e5mCEKLBLaMT6fRdSQZpg9CCl70+qO/F/spL2EmV8Dzkc59Zdy142o+aYtdrpltyaT
8OkDXbiMRuh4Gw4U5+xlqaSsvDem8k0kpS04LkAfxKQHKBn9jPqyiqE53Wg1H6VlToJpInm58L/x6HLPd6r4ESbCSHMINXz/925zjDz+H0pnE4lVf5tILg==


Data Signature: ITEzN1gcInTrELjeRCl08biS9256OOZ1B/zH9iUKN1TAys3iilB/PnCOdk24/WiQW+wNrJMqIAprlIQOli8koPiZZcbg4yvmdB2fOq+z
qxGuMblOMszIwg40Nveg7fbFBwvyD/4ParSXUMrxXRv3EtUjgWn50OsdVILiw2cqr1m6tPz4qfNx6Z5stJzsZ2HqJNmd1N/XNKN+ydVPUWoY7/hWSSUiuQF0
6Ph6Bn9nUK7slwd36AIvtXJnqiRC8IeY1ypG8bj3rs5m4ZJynSEDHkqZyIsU9ID/m1zZ+b39n0fMl8VVWJYk57YeWQrYL+JQwtFSfX0Tx0g2eiOof5MPVw==
```

Εικόνα 4.8: Η εκτέλεση του mobile agent στον Host B

Βήμα 3: Αποκρυπτογράφηση με το ιδιωτικό κλειδί του B και έλεγχος ψηφιακής υπογραφής με το δημόσιο κλειδί του A

- Εκτέλεση στον Host B της εφαρμογής Host_B.java
- Διάβασμα αρχείων data_sig.txt (ψηφιακή υπογραφή) και enc_data.txt (κρυπτογραφημένα δεδομένα). Εμφάνιση του μνήματος και έλεγχος της ακεραιότητας των δεδομένων και της ψηφιακής υπογραφής του αποστολέα.

```
C:\Users\George Hadjikyriacou\Google Drive\Private\Portfolio\Documents\ΑΠΚΥ - MSc\3ο Εξάμηνο - Διατριβή Μάστερ\Master Th
esis\Aglets Test\HostSoftware\Host_B_Reader>java Host_B 123456b b654321

Sun Feb 17 08:32:22 EET 2019 - CONFIDENTIAL INFO: Superman is Clark Kent!

Signature correct: true
```

Εικόνα 4.6: Η αποκρυπτογράφηση στον Host B

Αρχείο καταγραφής συμβάντων (Log File)

Στον Host B τηρείται αρχείο καταγραφής συμβάντων (Log.txt). Ο λόγος ύπαρξης αυτού του αρχείου είναι για σκοπούς παρακολούθησης, ανάλυσης και εξαγωγής συμπερασμάτων, όπως για παράδειγμα αν έγινε απόπειρα «παρενόχλησης» του mobile agent.

Στο αρχείο γίνεται η καταγραφή των παρακάτω:

- Καταγραφή ημερομηνία/ώρας αποστολής (dispatch) και επιστροφής (arrival). Σε περίπτωση που δεν επιστρέψει ο mobile agent ίσως έχει συμβεί κάτι κακόβουλο.
- Καταγραφή χρόνου αποστολής και επιστροφής (round trip). Σε περίπτωση που καθυστερήσει ο mobile agent ίσως έχει συμβεί κάτι κακόβουλο. Σε αυτή την περίπτωση πρέπει να λάβουμε υπόψιν μας τους συνήθης χρόνους εκτέλεσης, όπως επίσης και την κίνηση του δικτύου.
- Καταγραφή της επαλήθευσης της ακεραιότητας των δεδομένων (ψηφιακής υπογραφής). Σε περίπτωση που δεν καταφέρουμε να επαληθεύσουμε την ακεραιότητα των δεδομένων που μεταφέρει ο mobile agent ή την ψηφιακή υπογραφή του αποστολέα (Signature correct: false) ίσως έχει συμβεί κάτι κακόβουλο.

Στιγμιότυπο από το αρχείο καταγραφής:

```
[…]
Fri Feb 15 22:01:41 EET 2019(Aglet) | Aglet 1f1e30aa8677f239 created
Fri Feb 15 22:01:41 EET 2019(Aglet) | Aglet 1f1e30aa8677f239 dispatched
Fri Feb 15 22:01:41 EET 2019(Aglet) | Aglet 1f1e30aa8677f239 picked the data
Fri Feb 15 22:01:41 EET 2019(Aglet) | Aglet 1f1e30aa8677f239 arrived | Round Trip:
281ms
Fri Feb 15 22:02:15 EET 2019(Reader) | Signature correct: true
[…]
```

Εδώ να σημειωθεί ότι πρέπει να γίνεται αυτόματος συγχρονισμός των ρολογιών όλων των hosts μέσω του time server (NTP) της Microsoft time.windows.com (policy 0012). Αυτό πρέπει να γίνεται, για να μην υπάρχουν χρονικές διαφορές στο αρχείο καταγραφής.

Η ποιο πάνω δοκιμή συμμορφώνεται με τις παρακάτω πολιτικές και διαδικασίες του ΣΔΑΠ:

- Πολιτική 010: Χρήση κρυπτογράφησης
- Πολιτική 012: Τήρηση αρχείων καταγραφής συμβάντων
- Πολιτική 016: Ασφάλεια στην ανάπτυξη λογισμικού
- Διαδικασία 008: Κύκλος ζωής λογισμικού

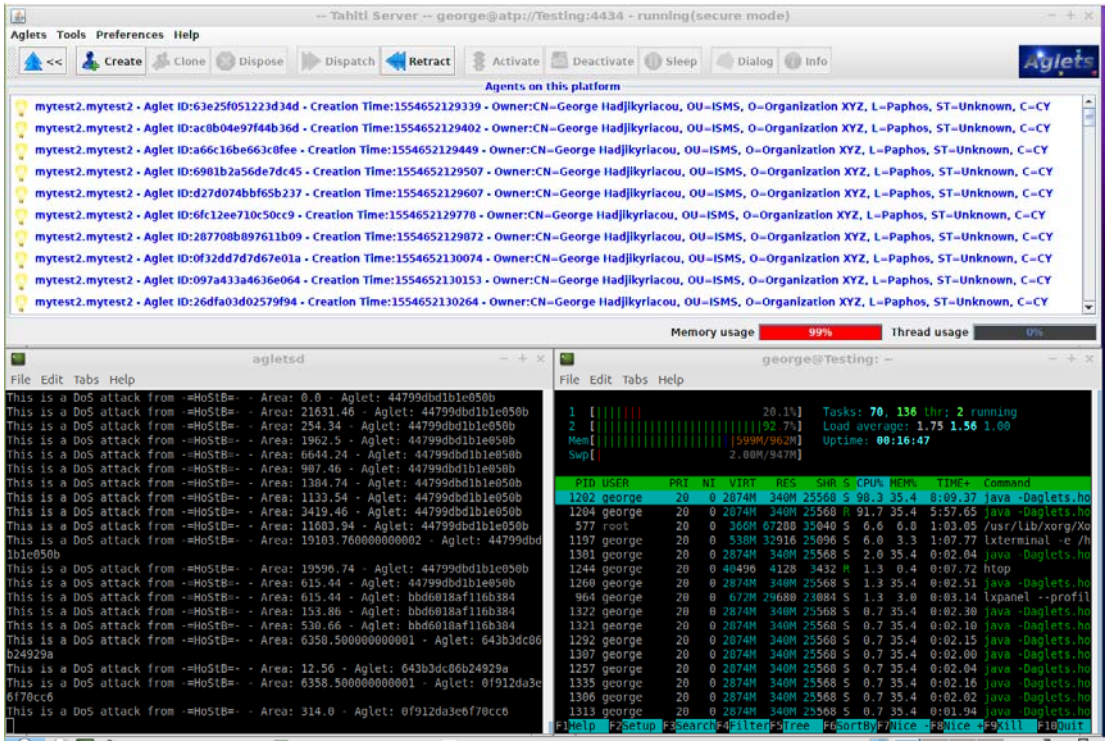
Δεν συμμορφώνεται με την πολιτική 009 μιας και οι κωδικοί που χρησιμοποιήσαμε είναι αδύνατοι.

4.5 Μελέτη περίπτωσης 4: Ασφάλεια Πλατφόρμας Mobile Agent – Επίθεση Άρνησης Υπηρεσίας (DoS Attack)

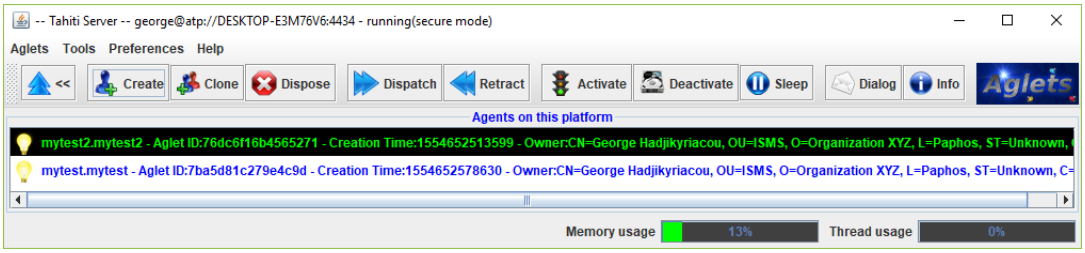
Σε αυτή την μελέτη περίπτωσης θα μελετήσουμε πως το ISO 27001 μπορεί να βοηθήσει στην προστασία της πλατφόρμας mobile agents από επιθέσεις άλλων πρακτορείων και συγκεκριμένα από επιθέσεις τύπου DoS (Denial of Service Attack). Για την δοκιμή χρησιμοποιήσαμε τους Host από την Μελέτη Περίπτωσης 3 (Εικόνα 4.5).

Για αυτό τον σκοπό δημιουργήσαμε έναν mobile agent (**Παράρτημα Θ – Θ.4**) ο όποιος έχει ως «αποστολή» να μεταφερθεί σε έναν host και στην συνέχεια να δημιουργεί ασταμάτητα κλώνους (δώσαμε το σχετικό δικαίωμα στο αρχείο aglets.policy) που θα εκτελούν επίσης ασταμάτητα μια μαθηματική πράξη με τυχαίους αριθμούς και επιπλέον θα δεσμεύει μνήμη γεμίζοντας ένα Vector. Την μαθηματική πράξη θα την εκτελεί για δέσμευση επεξεργαστικής ισχύς, ενώ το Vector θα το γεμίζει για δέσμευση της μνήμης RAM, γεμίζοντάς την με άχρηστα δεδομένα. Επιπλέον, όπως θα δούμε πιο κάτω στην Εικόνα 4.9 δεσμεύεται και αποθηκευτικός χώρος στον σκληρό δίσκο, για τον λόγο ότι η έξοδος της εκτέλεσης του mobile agent καταγράφεται και στο αρχείο καταγραφής συμβάντων (aglets.log).

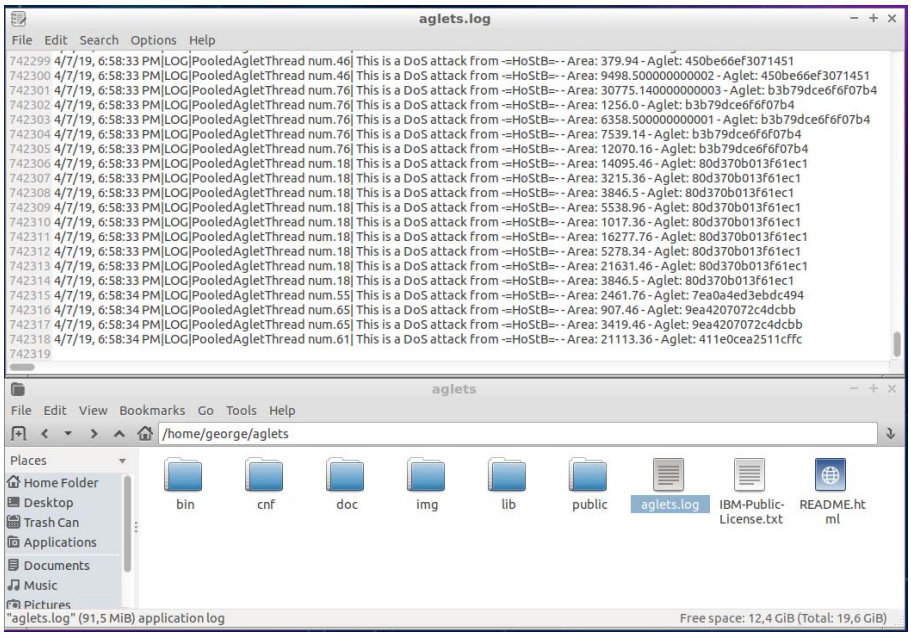
Αφού τρέξαμε για **10 λεπτά** τον κακόβουλο κώδικα στον Host A, βλέπουμε στην Εικόνα 4.7 ότι η ελεύθερη μνήμη της πλατφόρμας βρίσκεται στο 1%, και ο επεξεργαστής καθυστερεί στην εκτέλεση άλλων διεργασιών (load average >1.0). Αυτό το παρατηρήσαμε και όταν προσπαθήσαμε να εκτελέσουμε άλλους mobile agents στον Host A (Εικόνα 4.8), όπου δεν έγινε εφικτή η εκτέλεση τους. Τέλος, στην Εικόνα 4.9 βλέπουμε το αρχείο καταγραφής της πλατφόρμας, το οποίο κατά την διάρκεια της επίθεσης, έχει καταγράψει 742318 συμβάντα και έχει μέγεθος >91MB.



Εικόνα 4.7: Εκτέλεση του κακόβουλου mobile agent.



Εικόνα 4.8: Άρνηση εκτέλεσης άλλων mobile agents από τον Host B



Εικόνα 4.9: το αρχείο καταγραφής συμβάντων της πλατφόρμας Aglets

Στο Κεφάλαιο 3 υλοποιήσαμε πολιτικές και διαδικασίες ώστε να προστατεύεται ένα πρακτορείο από εκτέλεση κακόβουλων mobile agents. Συγκεκριμένα:

- Στην Διαδικασία 007 υποχρεώνει το πρακτορείο που θέλει να εκτελέσει κώδικα, να δεσμευθεί νομικά ότι δεν θα προβεί σε καμία κακόβουλη ενέργεια εναντίων του πρακτορείου του οργανισμού XYZ και ότι δέχεται να επιθεωρείται ο κώδικας και το ΣΔΑΠ από το άλλο μέρος σε τακτά χρονικά διαστήματα (Συμβόλαιο 002). Οποιαδήποτε κακόβουλη ενέργεια ή η μη τήρηση του συμβολαίου, έχει ως αποτέλεσμα τον τερματισμό της συνεργασίας η/και την λήψη νομικών μέτρων και αποζημιώσεων.
- Η καταγραφή συμβάντων (Πολιτική 012) θα βοηθήσει στην παρακολούθηση των ενεργειών των mobile agents, στην έγκαιρη ανίχνευση κακόβουλης ενέργειας, αλλά μπορεί να χρησιμοποιηθούν και ως αποδεικτικά στοιχεία σε περίπτωση λήψης νομικών μέτρων.
- Επίσης, η διαδικασία αξιολόγησης πρακτορείων (Διαδικασία 007) μας βοηθά να επιλέξουμε ποια πρακτορεία θα μπορούν να εκτελούν κώδικα στους hosts του οργανισμού μας και με ποια δικαιώματα.

Κεφάλαιο 5

Αποτελέσματα & Συμπεράσματα

5.1 Απαντήσεις στα ερευνητικά ερωτήματα

Όπως είδαμε, στο Κεφάλαιο 2, μελετήσαμε τους διάφορους τύπους επιθέσεων που μπορεί να δεχτούν οι mobile agents όπως παρουσιάζονται από τους ερευνητές στην διεθνή βιβλιογραφία. Μελετώντας την βιβλιογραφία καθορίσαμε επίσης και τις ανάγκες για ασφάλεια στους mobile agents που δεν είναι άλλες από την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων που μεταφέρει, απαντώντας με αυτό τον τρόπο το πρώτο ερευνητικό ερώτημα που θέσαμε, δηλαδή ποιες είναι οι ανάγκες για ασφάλεια στους mobile agents.

Χρησιμοποιώντας ως βάση αυτούς τους κινδύνους, προχωρήσαμε στο Κεφάλαιο 3 και στην υλοποίηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών ενός οργανισμού-μοντέλο, που συμμορφώνεται πλήρως με τις απαιτήσεις του διεθνούς προτύπου ISO 27001:2013. Στην δημιουργία του ΣΔΑΠ, συνέβαλε η εκπαίδευση αλλά και η επαγγελματική εμπειρία του ερευνητή.

Μέσα από την διαδικασία της διαχείρισης των κινδύνων, διαπιστώσαμε ότι οι κίνδυνοι των mobile agents δεν περιορίζονται μόνο σε κακόβουλες επιθέσεις που προέρχονται από άτομα εκτός του οργανισμού, αλλά και από άτομα και καταστάσεις εντός του οργανισμού καθώς επίσης από φυσικές καταστροφές.

Τον τρόπο με τον οποίο αντιμετωπίσαμε αυτούς τους κινδύνους μας τον έδωσε το ίδιο το πρότυπο, στο Παράρτημα Α, όπου δίνονται 144 έλεγχοι ασφαλείας. Με αυτούς τους ελέγχους, δημιουργήσαμε πολιτικές και διαδικασίες που αν τηρηθούν από το προσωπικό του οργανισμού, διασφαλίζεται μεταξύ άλλων περιουσιακών στοιχείων και η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των mobile agents.

Στο Κεφάλαιο 4 μελετήσαμε ορισμένες ρεαλιστικές περιπτώσεις που μας βοήθησαν να απαντήσουμε θετικά στα αλλά δύο ερευνητικά ερωτήματα που θέσαμε, δηλαδή αν:

- Οι απαιτήσεις του πρότυπου ISO 27001 θα μπορούσαν να παρέχουν ένα επιπλέον επίπεδο προστασίας στα δεδομένα που μεταδίδονται μέσω των mobile agents.
- Η δημιουργία και η εφαρμογή κατάλληλων πολιτικών ασφαλείας και διαδικασιών από τους προγραμματιστές και διαχειριστές συστημάτων, θα μπορούσαν να αποτρέψουν την εκτέλεση κακόβουλου λογισμικού ή/και τη διαρροή ευαίσθητων πληροφοριών από τους mobile agents σε μη εξουσιοδοτημένα άτομα.

Ας δούμε όμως πιο αναλυτικά, με ποιο τρόπο παρέχεται αυτό το επιπλέον επίπεδο ασφαλείας στις περιπτώσεις που μελετήσαμε:

Μελέτη Περίπτωσης 1:

Σε αυτή την περίπτωση βλέπουμε τις διορθωτικές ενέργειες που ακολουθεί ο διευθυντής ασφάλειας πληροφοριών μετά από την ενημέρωσή του για το κενό ασφαλείας στην πλατφόρμα Aglets.
Μόλις αντιληφθεί ότι η πλατφόρμα είναι ευάλωτη στο κενό ασφαλείας, ενημερώνει τον προμηθευτή ώστε να προβεί σε διόρθωση του κενού ασφαλείας. Στην πορεία διαπιστώνει ένα επιπλέον πρόβλημα που έχει να κάνει με την μη εφαρμογή της πολιτικής 009 από τον υπεύθυνο της πλατφόρμας Aglets και κατά συνέπια την μη συμμόρφωση με το πρότυπο και συγκεκριμένα με τον έλεγχο ασφαλείας Α.9.4, αλλά και την αλλαγή των προκαθορισμένων από τον κατασκευαστή στοιχείων πρόσβασης (Διαδικασία 005).
Βλέπουμε, ότι χρησιμοποίησε τεχνικές ελέγχου παρείσφρησης (penetration testing) για να μετρήσει την αποδοτικότητα του ΣΔΑΠ (Παράγραφος 9.1) και στην συνέχεια ιεράρχησε την λύση των προβλημάτων ξεκινώντας από το πιο σοβαρό. Πρώτα ξεκίνησε στην ενημέρωση του προμηθευτή για το κενό ασφαλείας στην πλατφόρμα, ώστε να δρομολογηθεί η λύση του, μετά προχώρησε με την άμεση αλλαγή του κωδικού της πλατφόρμας με έναν πιο δυνατό και στην συνέχεια ασχολήθηκε με την επιβολή πειθαρχικών μέτρων στον υπεύθυνο της πλατφόρμας. Η λήψη πειθαρχικών μέτρων, πέρα από το γεγονός ότι είναι απαίτηση του προτύπου (έλεγχος Α.7.2.3) αποτελεί και ένα κίνητρο ώστε να τηρούνται οι πολιτικές ασφαλείας από όλο το προσωπικό.
Τέλος, με την ενημέρωση του εγγράφου της πολιτικής 010, γίνεται συμμόρφωση με την τελευταία παράγραφο του προτύπου (10.2), που αφορά την συνεχή βελτίωση του ΣΔΑΠ.

Με αυτό τον τρόπο διασφαλίζουμε ότι λάθη που έγιναν δεν θα επαναληφθούν στο μέλλον και ότι λαμβάνουμε τα κατάλληλα μέτρα για την ασφάλεια των εφαρμογών που αναπτύσσει ο οργανισμός.

Μελέτη περίπτωσης 2:

Σε αυτή την περίπτωση μπορούμε να αντιληφθούμε τα προβλήματα που πιθανόν να δημιουργηθούν σε έναν οργανισμό αν δεν υπάρχουν και δεν τηρούνται πολιτικές και διαδικασίες ασφαλείας.
Η ελλιπής φυσική ασφάλεια των εγκαταστάσεων, σε συνδυασμό με την μη ύπαρξη δεσμευτικών εργασιακών συμβολαίων και συμφώνων εμπιστευτικότητας, έφεραν καταστροφικά αποτελέσματα στον οργανισμό. Στον Πίνακα 5.1 (Μελέτη περίπτωσης 2) βλέπουμε τις απαιτήσεις του προτύπου που θα βοηθήσουν ώστε παρόμοια προβλήματα μα μην επαναληφθούν στο μέλλον.

Μελέτη περίπτωσης 3:

Στην 3η περίπτωση που μελετήσαμε, είδαμε έναν ασφαλή τρόπο μεταφοράς δεδομένων με την χρήση του αλγόριθμου κρυπτογράφησης δημοσίου κλειδιού RSA, τηρώντας με αυτό τον τρόπο την πολιτική 010. Αυτό που πετύχαμε ήταν το τρίπτυχο εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα, λαμβάνοντας υπόψιν μας τον σχεδιασμό επιχειρησιακής συνέχειας που υλοποιήσαμε στον σχεδιασμό 001.
Την εμπιστευτικότητα την πετύχαμε κρυπτογραφώντας το μήνυμά μας με έναν ισχυρό αλγόριθμο κρυπτογράφησης όπως είναι ο RSA, την ακεραιότητα τον δεδομένων την πετύχαμε με την επαλήθευση της ψηφιακής υπογραφής του μνήματος, ενώ την διαθεσιμότητα την πετύχαμε με την εγκατάσταση UPS, συστήματος RAID αλλά και το τακτικά αντίγραφα ασφαλείας. Επίσης, πετύχαμε και την επαλήθευση του αποστολέα (non repudiation), μιας και το μήνυμα έχει υπογραφεί ψηφιακά με το ιδιωτικό του κλειδί. Για να αποφύγουμε την πιθανότητα κάποιος κακόβουλος να στείλει άλλο δημόσιο κλειδί σε έναν από τους δυο hosts (man in the middle attack), σωστό θα ήταν να χρησιμοποιηθεί μια τρίτη έμπιστη αρχή που σαν σκοπό θα έχει την πιστοποίηση της εγκυρότητας των δημοσίων κλειδιών των δυο Host. Να γίνει χρήση δηλαδή Υποδομής Δημοσίου Κλειδιού ή PKI (Public key Infrastructure)[37].

Οι λόγοι που στην πολιτική 010 επιλέξαμε τους αλγόριθμους AES, RSA και EEC είναι [37]:

- Είναι και οι τρεις ισχυροί αλγόριθμοι κρυπτογράφησης.
- Ο AES είναι σχεδιασμένος με τέτοιο τρόπο, ώστε να είναι ανθεκτικός γνωστών κρυπταναλυτικών τεχνικών και μπορεί επίσης να υλοποιηθεί εύκολα σε επεξεργαστές 8bit.
- Η ασφάλεια του RSA βασίζεται στο πρόβλημα της παραγοντοποίησης μεγάλων ακεραίων αριθμών (factorization problem), που μέχρι αυτή την στιγμή, δεν υπάρχει μέθοδος αποδοτικής λύσης του.
- Όπως και στον RSA έτσι και η ασφάλεια των αλγόριθμων ελλειπτικών καμπυλών βασίζεται σε δύσκολα μαθηματικά προβλήματα.

Περιορισμοί RSA:

Στο πιο πάνω παράδειγμα και για σκοπούς δοκιμής, χρησιμοποιήσαμε τον αλγόριθμο κρυπτογράφησης RSA με κλειδί (k) μεγέθους 2048 bits (256 bytes). Ο συγκεκριμένος αλγόριθμος έχει περιορισμό ως προς το μέγεθος του μηνύματος (mLen) που μπορεί να κρυπτογραφηθεί [30].

Ισχύει:
mLen <= k – 11 bytes (για το minimum padding PKCS#1 v.1.5), οπότε μπορούμε να κρυπτογραφήσουμε δεδομένα μέγιστου μεγέθους 245 bytes (256 - 11)

Τα Padding bits είναι τυχαία bits που προθέτονται στο μήνυμα που θέλουμε να κρυπτογραφήσουμε ώστε να είναι ασφαλές σε επιθέσεις «επιλεγμένου κρυπτοκειμένου» (chosen ciphertext attack) [37].

Για μεγαλύτερου μεγέθους δεδομένα θα μπορούσαμε να χρησιμοποιήσουμε τον AES για την κρυπτογράφηση των δεδομένων και τον RSA για κρυπτογράφηση του κλειδιού του AES (ο οποίος μπορεί να παράγεται τυχαία, αρκεί να ακολουθεί τις οδηγίες της πολιτικής 009).

Μελέτη περίπτωσης 4:

Στην 4η περίπτωση υλοποιήσαμε μία επίθεση τύπου άρνησης υπηρεσίας (Denial of Service Attack) στην πλατφόρμα Aglets. Η επίθεση είχε ως σκοπό να πλήξει την διαθεσιμότητα της πλατφόρμας Aglets δεσμεύοντας επεξεργαστική ισχύ (CPU), μνήμη (RAM) και αποθηκευτικό χώρο (HDD). Το πείραμα πέτυχε μιας και μετά από 10 λεπτά και κατά την διάρκεια της επίθεσης, προσπαθήσαμε να στείλουμε και άλλους mobile agents στον host που δεχόταν την επίθεση για εκτέλεση, αλλά χωρίς αποτέλεσμα.

Την συγκεκριμένη επίθεση την αντιμετωπίζουμε με δυο τρόπους στο ΣΔΑΠ που δημιουργήσαμε:

- **Τεχνικά** – Με την εφαρμογή ενός συστήματος ανίχνευσης εισβολέων (Intrusion Detection System ή IDS). Ένα τέτοιο σύστημα για την πλατφόρμα Aglets, αναλύεται στην μελέτη των Giovani Vigna, Bryan Cassell και Dave Fayram [38] όπου επεκτείνουν την πλατφόρμα Aglets ώστε να παράγει πληροφορίες ελέγχου (auditing information), που αφορούν τις ενέργειες των mobile agents. Στην συνέχεια αναλύοντας αυτές τις πληροφορίες η προσέγγιση τους είναι σε θέση να ανιχνεύσει διάφορων τύπων επιθέσεις.
- **Οργανωτικά** – Με την σύναψη συμφωνιών μεταξύ πρακτορείων όπου τα δύο μέρη, θα δεσμεύονται νομικά ότι δεν θα προβούν σε κακόβουλες ενέργειες εναντίον του άλλου πρακτορείου. Επιπλέον, τα πρακτορεία θα μπορούν να δίνουν το δικαίωμα το ένα στο άλλο ώστε να διενεργούν τακτικές επιθεωρήσεις (του κώδικα ή/και του ΣΔΑΠ). Το ISO 27001 με τον έλεγχο A.18.1.1 απαιτεί από τον οργανισμό να αναγνωρίσει τις απαιτήσεις της νομοθεσίας αλλά και των συμβολαίων. Τις απαιτήσεις της νομοθεσίας τις καθορίζει το εκάστοτε κράτος (Πολιτική 007), ενώ τις απαιτήσεις των συμβολαίων ο εκάστοτε οργανισμός (Συμβόλαιο 002). Επιπλέον, η απαίτηση του ISO 27001 A.12.4 (Καταγραφή συμβάντων και παρακολούθηση) βοηθά τον οργανισμό ώστε να συλλέξει στοιχεία που να αποδεικνύουν την επίθεση εναντίον του.

Συνοπτικά:

Μελέτη Περίπτωσης	Απαίτηση του ISO 27001

1	• Α.7.2.3 Ύπαρξη πειθαρχικής διαδικασίας • Α.9.4.3 Χρήση ποιοτικών κωδικών πρόσβασης • Α.13.1.2 Υπογραφή συμφωνιών επιπέδου υπηρεσίας (SLA) • Παράγραφος 7.4 Επικοινωνία • Παράγραφος 9.1 Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση • Παράγραφος 10.1 Λήψη διορθωτικών ενεργειών σε περίπτωση μη συμμορφώσεων • Παράγραφος 10.2 Συνεχής βελτίωση του ΣΔΑΠ
2	• Α.7.2.3 Ύπαρξη πειθαρχικής διαδικασίας • Α.11 Φυσική και περιβαλλοντική ασφάλεια • Α.11.2.9 Πολιτική καθαρού γραφείου/καθαρής οθόνης • Α.13.2.4 Υπογραφή συμφώνων εμπιστευτικότητας από το προσωπικό και τους συνεργάτες. • Α.14.2 Ασφάλεια στην ανάπτυξη λογισμικού • Α.16.1 Διαχείριση περιστατικών ασφάλειας πληροφοριών • Α.18.1 Συμμόρφωση με τις απαιτήσεις της νομοθεσίας και των συμβολαίων.
3	• Α.6.1.5 Ασφάλεια πληροφοριών στην διαχείριση έργων. • Α.10.1 Κρυπτογραφικοί έλεγχοι και διαχείριση κλειδιών. • Α.12.4 Καταγραφή συμβάντων και παρακολούθηση • Α.12.4.4 Συγχρονισμός ρολογιών • Α.14.2 Ασφάλεια στην ανάπτυξη λογισμικού • Α.17 Επιχειρησιακή Συνέχεια Ασφάλειας Πληροφοριών
4	• Α.12.4 Καταγραφή συμβάντων και παρακολούθηση • Α.18.1 Συμμόρφωση με τις απαιτήσεις της νομοθεσίας και των συμβολαίων.

Πίνακας 5.1: Απαιτήσεις του ISO 27001 που συμβάλουν στην ασφάλεια των mobile agents

Όπως βλέπουμε, το πρότυπο καθοδηγεί με τέτοιο τρόπο το άτομο που θα υλοποιήσει το ΣΔΑΠ, ώστε να εφαρμοστεί η μέγιστη δυνατή ασφάλεια των δεδομένων ενός οργανισμού σε όλα τα επίπεδα, από τον σχεδιασμό της φυσικής ασφάλειας, την εκπαίδευση του προσωπικού, μέχρι τον τρόπο που συνάπτει συμφωνίες και εφαρμόζει τους τεχνικούς ελέγχους.

Διαπιστώνουμε ότι μέσα από απαιτήσεις του προτύπου όπως για παράδειγμα: α) η διαχείριση κινδύνων (Παράγραφοι 6.1.2 και 6.1.3), β) ο καθορισμός και η τήρηση πολιτικών ασφαλείας (Α.5.1.1), γ) η ευαισθητοποίηση και ενημέρωση του προσωπικού (Παράγραφος 7.3), δ) η διαδικασία εσωτερικού ελέγχου τους ΣΔΑΠ (Παράγραφος 9.2) αλλά και ε) η συνεχής βελτίωση του ΣΔΑΠ (Παράγραφος 10.2), το πρότυπο ISO 27001 μπορεί να προσθέσει ένα επιπλέον επίπεδο προστασίας στους mobile agents και τις πλατφόρμες τους.

Τέλος, ένα σύστημα διαχείρισης ασφάλειας πληροφοριών δεν αποτελεί μια σειρά από στατικά έγγραφα, τα οποίο τοποθετούνται σε μία βιβλιοθήκη ή ένα συρτάρι χωρίς να γίνονται αλλαγές σε αυτά. Αντιθέτως, μέσα από την σωστή εφαρμογή των απαιτήσεων του, έχει την δυνατότητα να γίνει αποτελεσματικότερο και σε βάθος χρόνου να προσαρμοστεί απόλυτα στις ανάγκες ενός οργανισμού παρέχοντας ασφάλεια στα δεδομένα του. Καλλιεργεί την ανάλογη κουλτούρα στο προσωπικό του και εξασφαλίζει την εμπιστοσύνη από τους εξωτερικούς συνεργάτες και τους πελάτες του.

5.2 Περιορισμοί Έρευνας

Στην παρούσα διατριβή είχαμε τους εξής περιορισμούς:

- Δεν καταφέραμε να εφαρμόσουμε το σύστημα διαχείρισης ασφάλειας πληροφοριών που υλοποιήσαμε στο Κεφάλαιο 3 σε πραγματικό περιβάλλον. Αυτό πέρα από τον περισσότερο χρόνο και κόστος που θα απαιτούσε, θα μας ήταν δύσκολο να βρούμε οργανισμό με το συγκεκριμένο πεδίο εφαρμογής για να λάβουμε σχετική ανατροφοδότηση. Παρόλα αυτά χρησιμοποιήσαμε ορισμένα

ρεαλιστικά σενάρια στο Κεφάλαιο 4, για να αποδείξουμε τον τρόπο με τον οποίο το διεθνές πρότυπο ISO 27001 προσφέρει ένα επιπλέον επίπεδο ασφάλειας στους mobile agents.

- Για την σωστή υλοποίηση και εφαρμογή του ΣΔΑΠ απαιτείται η εμπλοκή όλου του προσωπικού ενός οργανισμού, που αρκετές φορές τα καθήκοντα τους πέρα από τις γνώσεις πληροφορικής, απαιτούν πιο εξειδικευμένες γνώσεις, εκπαίδευση ή σπουδές (π.χ. Διοίκηση επιχειρήσεων, Νομική, Διαχείριση Ανθρώπινου Δυναμικού, Ελεγκτική, κ.α.). Στην παρούσα εργασία ασχοληθήκαμε με τα απολύτως απαραίτητα καθήκοντα του προσωπικού για την δημιουργία του ΣΔΑΠ (διαδικασιών, πολιτικών, συμβολαίων, κ.α.). Σε πραγματικό περιβάλλον και για μεγαλύτερους οργανισμούς, τα έγγραφα αυτά πιθανόν να είναι πιο πολύπλοκα και με μεγαλύτερη λεπτομέρεια.
- Λόγο έλλειψης χρόνου δεν καταφέραμε να υλοποιήσουμε μια εφαρμογή που ο σκοπός της θα ήταν να αναλύει τα αρχεία καταγραφής συμβάντων της μελέτης περίπτωσης 3 για τυχόν κακόβουλες παρενοχλήσεις του mobile agent. Αυτό φυσικά αν και ξεφεύγει λίγο από το θέμα της διατριβής, θα μπορούσε να είναι αντικείμενο μελλοντικής μελέτης.

5.3 Μελλοντική μελέτη

Χρησιμοποιώντας ως βάση τον οργανισμό μοντέλο που δημιουργήσαμε και για το συγκεκριμένο πεδίο εφαρμογής, θα μπορούσαμε στο μέλλον να μελετήσουμε τα παρακάτω:

- Την υλοποίηση κανόνων ηθικής για mobile agents που χρησιμοποιούν τεχνητή νοημοσύνη.
- Την ενσωμάτωση των απαιτήσεων του Γενικού Κανονισμού της Ε.Ε για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα (GDPR) στο ΣΔΑΠ που δημιουργήσαμε.
- Την υλοποίηση άλλων διεθνών προτύπων που θα ενισχύσουν τον οργανισμό αλλά και την ασφάλεια των υπηρεσιών που παρέχει. Ένα τέτοιο πρότυπο μπορεί να είναι το ISO 22301 που παρέχει τις απαιτήσεις για συστήματα διαχείρισης της επιχειρηματικής συνέχειας (Business Continuity Management System ή BCMS).

Βιβλιογραφία

[01] Zaki Brahmi, Amine Lini, και Mohamed Mohsen Gammoudi – «Mobile Agent Security Based on Artificial Immune System», 2014

[02] Hind Idrissi, El Mamoun Souidi και Arnaud Revel – «Security of Mobile Agent Platforms Using Access Control and Cryptography», 2015

[03] Héla Hachicha, Donies Samet και Khaled Ghedira - «A Conceptual Approach to Place Security in Systems of Mobile Agents», 2015

[04] Axel Bürkle, Alice Hertel, Wilmuth Müller και Martin Wieser – «Evaluating the security of mobile agent platform», 2009

[05] Donies Samet, Farah Barika Ktata και Khaled Ghedira – «Security and Trust on Mobile Agent Platforms: A Survey», 2017

[06] International Organization for Standardization – «International Standard ISO/IEC 27001:2013», 2013

[07] European Commission - Information System Security Policy – «STANDARD ON MOBILE CODE», 2011

[08] Aglets Development Group – «The Aglets 2.0.2 User's Manual», 2009

[09] J. Baumann – «Mobile Agents: Control Algorithms», 2000

[10] Jiannong Cao και Sajal K. Das – «Mobile Agents in Networking and Distributed Computing», 2012

[11] ISO 27001 Details History and Structure [Online], Διαθέσιμο: https://cvgstrategy.com/iso-27001-details/ [Πρόσβαση: 21 Νοεμβρίου 2018]

[12] International Organization for Standardization [Online], Διαθέσιμο: https://www.iso.org [Πρόσβαση: 10 Νοεμβρίου 2018]

[13] International Organization for Standardization – «International Standard ISO/IEC 27003:2017», 2017

[14] SeMoA [Online], Διαθέσιμο: http://semoa.sourceforge.net/about/details.html [Πρόσβαση: 21 Νοεμβρίου 2018]

[15] Dejan Kosutic, «4 mitigation options in risk treatment according to ISO 27001» [Online], Διαθέσιμο: https://advisera.com/27001academy/blog/2016/05/16/4-mitigation-options-risk-treatment-according-iso-27001/ [Πρόσβαση: 8 Ιανουαρίου 2019]

[16] Jean Tajer, Mo Adda και Benjamin Aziz - «New Computing Model for Securing Mobile Agents in IP Networks», 2017

[17] ISO 27001 Academy [Online], Διαθέσιμο: https://advisera.com/27001academy/ [Πρόσβαση: 21 Νοεμβρίου 2018]

[18] SANS Institute - Information Security Policy Templates [Online], Διαθέσιμο: https://www.sans.org/security-resources/policies [Πρόσβαση: 21 Νοεμβρίου 2018]

[19] Planning for and Implementing ISO 27001 [Online], Διαθέσιμο: https://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Planning-for-and-Implementing-ISO27001.aspx [Πρόσβαση: 21 Νοεμβρίου 2018]

[20] Xavier Mertens (TrueSec) – «Penetration Test Agreement» [Online], Διαθέσιμο: https://www.scribd.com/document/281970301/TrueSec-Pentest-Agreement-v2-pdf

[21] Υποδείγματα ατομικών συμβάσεων εργασίας αορίστου χρόνου [Online], Διαθέσιμο: https://www.e-forologia.gr/cms/viewContents.aspx?id=203433 [Πρόσβαση: 20 Μαρτίου 2019]

[22] Aglets Software Development Kit [Online], Διαθέσιμο: https://sourceforge.net/projects/aglets/ Πρόσβαση: 21 Νοεμβρίου 2018

[23] Danny B. Lange και Mitsuru Oshima – «Programming and Deploying Java Mobile Agents Aglets », 1998

[24] Pankaj Kumar – «Chapter 3: Cryptography with Java » στο «J2EE™ Security for Servlets, EJBs and Web Services: Applying Theory and Standards to Practice», 2003

[25] Example of RSA generation, sign, verify, encryption, decryption and keystores in Java [Online], Διαθέσιμο: https://gist.github.com/nielsutrecht/855f3bef0cf559d8d23e94e2aecd4ede [Πρόσβαση: 20 Μαρτίου 2019]

[26] JKS private key cracker – Nail in the JKS coffin [Online], Διαθέσιμο: https://github.com/floyd-fuh/JKS-private-key-cracker-hashcat [Πρόσβαση: 20 Μαρτίου 2019]

[27] hashcat [Online], Διαθέσιμο: https://hashcat.net/hashcat/ [Πρόσβαση: 20 Μαρτίου 2019]

[28] Data Compliant GDPR CCTV Sign 200mm x 300mm - Rigid Plastic (CC.12F-RP) [Online], Διαθέσιμο: https://www.amazon.co.uk/Data-Compliant-GDPR-200mm-300mm/dp/B07JMW6YW7 [Πρόσβαση: 27 Μαρτίου 2019]

[29] No Video Photography Allowed Sign: No Photography, No Video Recording (K-0207) [Online], Διαθέσιμο: https://www.mysecuritysign.com/no-photography-no-video-recording-sign/sku-k-0207 [Πρόσβαση: 27 Μαρτίου 2019]

[30] PKCS #1: RSA Cryptography Specifications Version 2.2 [Online], Διαθέσιμο: https://tools.ietf.org/html/rfc8017 [Πρόσβαση: 29 Μαρτίου 2019]

[31] The ISO Survey [Online], Διαθέσιμο: https://www.iso.org/the-iso-survey.html [Πρόσβαση: 1 Απριλίου 2019]

[32] The ISO Survey (Data) [Online], Διαθέσιμο: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 [Πρόσβαση: 1 Απριλίου 2019]

[33] Business Continuity: 4 Steps to Take Before Knowledge leaves the building [Online], Διαθέσιμο: https://pecb.com/past-webinars/business-continuity-4-steps-to-take-before-knowledge-leaves-the-building [Πρόσβαση: 2 Απριλίου 2019]

[34] The SDLC: 7 phases, popular models, benefits & more [2019] [Online], Διαθέσιμο: https://raygun.com/blog/software-development-life-cycle/ [Πρόσβαση: 27 Μαρτίου 2019]

[35] Redundancy and Automated Alerts Ensure Business Continuity? [Online], Διαθέσιμο: https://www.smseagle.eu/2016/10/04/redundancy-and-automated-alerts-ensure-business-continuity/ [Πρόσβαση: 11 Απριλίου 2019]

[36] Double Door Airlock integrated with People Counter Sensor [Online], Διαθέσιμο: http://www.fingerprint-access-control.com/technology/double-door-airlock-interlock-mantrap/ [Πρόσβαση: 11 Απριλίου 2019]

[37] Κωνσταντίνος Λιμνιώτης - Διαφάνειες Διαλέξεων Θ.Ε ΑΥΔ-621 «Κρυπτογραφία», 2017

[38] Giovani Vigna, Bryan Cassell και Dave Fayram – «An Intrusion Detection System for Aglets», 2002

[39] The Chelsea Manning Case: A Timeline [Online], Διαθέσιμο: https://www.aclu.org/blog/free-speech/employee-speech-and-whistleblowers/chelsea-manning-case-timeline [Πρόσβαση: 17 Απριλίου 2019]

[40] Edward Snowden: Leaks that exposed US spy programme [Online], Διαθέσιμο: https://www.bbc.com/news/world-us-canada-23123964 [Πρόσβαση: 17 Απριλίου 2019]

[41] ESET Cybersecurity Awareness Training [Online], Διαθέσιμο: https://www.eset.com/us/cybertraining/ [Πρόσβαση: 26 Απριλίου 2019]

[42] Jennifer Rowley – «Using Case Studies in Research»,2002

Παράρτημα Α

Διαχείριση Κινδύνων

A.1 Περιουσιακά στοιχεία

Περιουσιακά Στοιχεία		
Περιουσιακό Στοιχείο	**Τύπος**	**Ιδιοκτήτης**
Διοίκηση	Προσωπικό	N/A
Διευθυντής Πληροφορικής	Προσωπικό	Τμήμα Πληροφορικής
Διαχειριστής Συστημάτων και Δικτύου	Προσωπικό	Τμήμα Πληροφορικής
Προγραμματιστής	Προσωπικό	Τμήμα Πληροφορικής
Διευθυντής Ασφάλειας Πληροφοριών	Προσωπικό	Τμήμα Πληροφορικής
Διευθυντής Ανθρώπινου Δυναμικού	Προσωπικό	Τμήμα Ανθρώπινου Δυναμικού
Νομικός Σύμβουλος	Προσωπικό	Νομικό Τμήμα
Διευθυντής Διαχείρισης Εγκαταστάσεων	Προσωπικό	Τμήμα Διαχείρισης Εγκαταστάσεων
Υπεύθυνος Φυσικής Ασφάλειας	Προσωπικό	Τμήμα Διαχείρισης Εγκαταστάσεων
Συνεργείο Καθαρισμού	Προσωπικό	Τμήμα Διαχείρισης Εγκαταστάσεων
Εσωτερικός Ελεγκτής	Προσωπικό	Τμήμα Εσωτερικού Ελέγχου
Workstation 1	Υλικό/Εξοπλισμός	Διαχειριστής Συστημάτων και Δικτύου
Workstation 2, 3	Υλικό/Εξοπλισμός	Προγραμματιστής
Workstation 4	Υλικό/Εξοπλισμός	Διευθυντής Ανθρώπινου Δυναμικού
Workstation 5	Υλικό/Εξοπλισμός	Νομικός Σύμβουλος
Workstation 6	Υλικό/Εξοπλισμός	Υπεύθυνος Φυσικής Ασφάλειας
Workstation 7	Υλικό/Εξοπλισμός	Διοίκηση
Workstation 8	Υλικό/Εξοπλισμός	Reception
Laptop 1	Υλικό/Εξοπλισμός	Εσωτερικός Ελεγκτής
Laptop 2	Υλικό/Εξοπλισμός	Διοίκηση
Printer 1	Υλικό/Εξοπλισμός	Διευθυντής Ανθρώπινου Δυναμικού
Printer 2	Υλικό/Εξοπλισμός	Νομικός Σύμβουλος
Printer 3	Υλικό/Εξοπλισμός	Εσωτερικός Ελεγκτής
Printer 4	Υλικό/Εξοπλισμός	Διοίκηση
Modem / Router / Firewall	Υλικό/Εξοπλισμός	Διαχειριστής Συστημάτων και Δικτύου
Backup NAS	Υλικό/Εξοπλισμός	Διαχειριστής Συστημάτων και Δικτύου
Switch	Υλικό/Εξοπλισμός	Διαχειριστής Συστημάτων και Δικτύου
Router 2	Υλικό/Εξοπλισμός	Προγραμματιστής
Production Hosts	Υλικό/Εξοπλισμός	Προγραμματιστής
SVN Server	Υλικό/Εξοπλισμός	Προγραμματιστής
Test Host 1	Υλικό/Εξοπλισμός	Προγραμματιστής
Test Host 2	Υλικό/Εξοπλισμός	Προγραμματιστής
Test Host 3	Υλικό/Εξοπλισμός	Προγραμματιστής
Workstation (1-8)	Υλικό/Εξοπλισμός	Ο εκάστοτε ιδιοκτήτης
Laptop (1-2)	Υλικό/Εξοπλισμός	Ο εκάστοτε ιδιοκτήτης
Test Host (1-3)	Υλικό/Εξοπλισμός	Προγραμματιστής
Printer (1-4)	Υλικό/Εξοπλισμός	Ο εκάστοτε ιδιοκτήτης
Κτιριακές Εγκαταστάσεις/ Γραφεία	Υλικό/Εξοπλισμός	Υπεύθυνος Φυσικής Ασφάλειας

Σύστημα Συναγερμού	Υλικό/Εξοπλισμός	Υπεύθυνος Φυσικής Ασφάλειας
Αντιπυρικό σύστημα	Υλικό/Εξοπλισμός	Υπεύθυνος Φυσικής Ασφάλειας
Αντιπλημμυρικό σύστημα	Υλικό/Εξοπλισμός	Υπεύθυνος Φυσικής Ασφάλειας
Κλειστό Κύκλωμα Τηλεόρασης (CCTV)	Υλικό/Εξοπλισμός	Υπεύθυνος Φυσικής Ασφάλειας
Καταστροφέας Εγγράφων	Υλικό/Εξοπλισμός	Υπεύθυνος Φυσικής Ασφάλειας
Καταστροφέας Μέσων Αποθήκευσης	Υλικό/Εξοπλισμός	Υπεύθυνος Φυσικής Ασφάλειας
Αποθηκευτικός Χώρος Εγγράφων & Μέσων Αποθήκευσης	Υλικό/Εξοπλισμός	Υπεύθυνος Φυσικής Ασφάλειας
Βαλίτσα Ασφαλείας Μεταφοράς Εγγράφων	Υλικό/Εξοπλισμός	Υπεύθυνος Φυσικής Ασφάλειας
Συμβόλαια / NDAs	Δεδομένα	Διοίκηση
Mobile Agents/Data	Δεδομένα	Προγραμματιστής
Mobile Agent Platform	Λογισμικό	Προγραμματιστής
Γλώσσα/Περιβάλλον Προγραμματισμού (IDE)	Λογισμικό	Προγραμματιστής
Πηγαίος Κώδικας	Δεδομένα	Προγραμματιστής
Λειτουργικά Συστήματα	Λογισμικό	Διαχειριστής Συστημάτων και Δικτύου
E-mail Clients	Λογισμικό	Ο εκάστοτε ιδιοκτήτης
Λογισμικό Anti-malware	Λογισμικό	Διαχειριστής Συστημάτων και Δικτύου
IPS/IDS	Λογισμικό	Διαχειριστής Συστημάτων και Δικτύου
Log File Analyzer	Λογισμικό	Διαχειριστής Συστημάτων και Δικτύου
Log File Analyzer (Mobile Agent Platform)	Λογισμικό	Προγραμματιστής
Δικτυακές καλωδιώσεις	Υλικό/Εξοπλισμός	Διαχειριστής Συστημάτων και Δικτύου
E-mails	Δεδομένα	Ο εκάστοτε ιδιοκτήτης
UPS	Υλικό/Εξοπλισμός	Διαχειριστής Συστημάτων και Δικτύου
Μέσα αποθήκευσης ψηφιακών δεδομένων	Υλικό/Εξοπλισμός	Διαχειριστής Συστημάτων και Δικτύου
Έγγραφα	Δεδομένα	Ο εκάστοτε ιδιοκτήτης
Πολιτικές Ασφαλείας/Διαδικασίες/Σχεδιασμοί	Δεδομένα	Ο εκάστοτε ιδιοκτήτης
Βιβλίο καταγραφής επισκεπτών	Δεδομένα	Υπεύθυνος Φυσικής Ασφάλειας
Εξουσιοδοτημένοι παραλήπτες περιουσιακών στοιχείων	Δεδομένα	Διευθυντής Ασφάλειας Πληροφοριών
Risk Assessment and Treatment	Δεδομένα	Διευθυντής Ασφάλειας Πληροφοριών
SoA	Δεδομένα	Διευθυντής Ασφάλειας Πληροφοριών
Αρχεια Καταγραφής (Αρχείο Καταγραφήςs)	Δεδομένα	Ο εκάστοτε ιδιοκτήτης

Α.2 Αξιολόγηση κινδύνων

Αξιολόγηση Κινδύνων					
Περιουσιακό Στοιχείο	**Ευπάθεια**	**Κίνδυνος**	**Επίπτωση**	**Πιθανότητα Εμφάνισης**	**Κίνδυνος**
Διοίκηση	Μη καθιέρωση / κοινοποίηση της πολιτικής και των στόχων ασφάλειας.	Ελλιπής ενημέρωση του προσωπικού και συνεργατών.	7	3	21
Διοίκηση	Μη παροχή απαραίτητων πόρων για εφαρμογή του ΣΔΑΠ.	Μη υλοποίηση του ΣΔΑΠ.	9	5	45
Διοίκηση	Μη τήρηση συμφωνιών/συμβολαίων	Νομικές και οικονομικές επιπτώσεις. Κακή φήμη. Διακοπή υπηρεσιών που παρέχεται από τρίτους.	9	2	18
Διοίκηση	Μη διενέργεια Ανασκόπησης Διοίκησης	Ελλιπής ενημέρωση σχετικά με την απόδοση του ΣΔΑΠ.	8	2	16
Διοίκηση	Ελλιπής ή μη καθορισμός ρόλων, ευθηνών και εξουσιών	Προβληματική ή μη εκτέλεση καθηκόντων από το προσωπικό	9	2	18
Διαχειριστής Συστημάτων και Δικτύου	Μη παρακολούθηση κίνησης δικτύου	Απώλεια της διαθεσιμότητας των δεδομένων	9	5	45
Διαχειριστής Συστημάτων και Δικτύου	Μη παρακολούθηση του Antivirus	Εκμετάλλευση ευπαθειών από Hacker. Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Διαχειριστής Συστημάτων και Δικτύου	Λανθασμένη ρύθμιση του Firewall & Web Content Filter	Εκμετάλλευση ευπαθειών από Hacker. Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Διαχειριστής Συστημάτων και Δικτύου	Μη τήρηση αντιγράφων ασφάλειας	Απώλεια της διαθεσιμότητας των δεδομένων	10	4	40
Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη ελέγχου χωρητικότητας	Απώλεια της διαθεσιμότητας των δεδομένων	10	3	30
Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη αναβάθμισης λογισμικού	Εκμετάλλευση ευπαθειών από Hacker. Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων	10	2	20
Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη εφαρμογής ελέγχων πρόσβασης στα συστήματα	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων	10	4	40
Διαχειριστής Συστημάτων και Δικτύου	Μη ανάλυση αρχείων καταγραφής (log files)	Αργοπορημένος εντοπισμός επίθεσης από Hacker	10	3	30

Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη καταγραφής και αναφοράς περιστατικών ασφάλειας	Νομικές και Οικονομικές Επιπτώσεις. Μη συμμόρφωση με το GDPR	8	2	16
Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη αντιμετώπισης περιστατικών ασφάλειας	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων	10	3	30
Διαχειριστής Συστημάτων και Δικτύου	Διακοπή ηλεκτρικού ρεύματος	Διακοπή επιχειρησιακών λειτουργειών του οργανισμού	8	3	24
Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη συντήρησης του εξοπλισμού	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων	10	2	20
Διαχειριστής Συστημάτων και Δικτύου	Απουσία λόγο ασθένειας	Δεν υπάρχει αντικαταστάτης	9	6	54
Προγραμματιστής	Παράλειψη ελέγχου της εφαρμογής, πριν την εκτέλεση της σε πραγματικές συνθήκες	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων	10	3	30
Προγραμματιστής	Μη τήρηση εκδόσεων του πηγαίου κώδικα	Μη δυνατότητα επαναφοράς του κώδικα σε προηγουμένη πιο σταθερή έκδοση	8	4	32
Προγραμματιστής	Μη εφαρμογή ελέγχων ασφαλείας κατά τον σχεδιασμό των εφαρμογών	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων των mobile agents	10	3	30
Διευθυντής Ασφάλειας Πληροφοριών	Έλλειψη συντονισμού των δραστηριοτήτων που αφορούν το ΣΔΑΠ	Μη τήρηση διαδικασιών που αφορούν την ασφάλεια	10	3	30
Διευθυντής Ανθρώπινου Δυναμικού	Πρόσληψη ακατάλληλα καταρτισμένου προσωπικού	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	5	50
Διευθυντής Ανθρώπινου Δυναμικού	Μη τήρηση διαδικασιών κατά την απόλυση προσωπικού	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	4	40
Διευθυντής Ανθρώπινου Δυναμικού	Ελλιπής ή καθόλου εκπαίδευση / ευαισθητοποίησης του προσωπικού σε θέματα ασφάλειας δεδομένων	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	6	60
Διευθυντής Ανθρώπινου Δυναμικού	Παράλειψη σύναψης συμφωνητικών εμπιστευτικότητας (NDAs) με προσωπικό, συνεργάτες / υπεργολάβους	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων. Νομικές, Οικονομικές επιπτώσεις. Κακή φήμη.	10	4	40
Νομικός Σύμβουλος	Παράλειψη προσδιορισμού απαιτήσεων για την συμμόρφωση του οργανισμού με την νομοθεσία	Νομικές, Οικονομικές επιπτώσεις. Κακή φήμη	10	2	20

Υπεύθυνος Φυσικής Ασφάλειας	Μη υλοποίηση ελέγχων για κλοπή / βιομηχανικής κατασκοπείας.	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	5	50
Υπεύθυνος Φυσικής Ασφάλειας	Μη υλοποίηση ελέγχων για φωτιά	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων	10	6	60
Υπεύθυνος Φυσικής Ασφάλειας	Μη υλοποίηση ελέγχων για πλημύρα	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων	10	4	40
Υπεύθυνος Φυσικής Ασφάλειας	Μη υλοποίηση ελέγχων για Σεισμό	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων	8	3	24
Συνεργείο Καθαρισμού	Κλοπή, Βιομηχανική κατασκοπεία	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων. Οικονομικές επιπτώσεις, Νομικά ζητήματα.	10	6	60
Συνεργείο Καθαρισμού	Καταστροφή εξοπλισμού (από λάθος ή από πρόθεση)	Απώλεια διαθεσιμότητας δεδομένων	10	5	50
Εσωτερικός Ελεγκτής	Παράλειψη διενέργειας εσωτερικού ελέγχου	Ελλιπής ή καθόλου ενημέρωση σχετικά με την απόδοση του ΣΔΑΠ και την συμμόρφωση με το πρότυπο ISO 27001	10	3	30
Workstation (1-8)	Κακόβουλο λογισμικό	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	6	60
Workstation (1-8)	Διακοπή ηλεκτρικού ρεύματος	Απώλεια διαθεσιμότητας των δεδομένων.	5	3	15
Workstation (1-8)	Καταστροφή από φωτιά	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	7	3	21
Workstation (1-8)	Καταστροφή από πλημύρα	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	7	3	21
Workstation (1-8)	Καταστροφή από σεισμό	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	7	2	14
Workstation (1-8)	Κλοπή	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	4	40
Laptop (1-2)	Κακόβουλο λογισμικό	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	6	60
Laptop (1-2)	Διακοπή ηλεκτρικού ρεύματος	Απώλεια διαθεσιμότητας των δεδομένων.	5	1	5

Laptop (1-2)	Καταστροφή από φωτιά	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	7	5	35
Laptop (1-2)	Καταστροφή από πλημύρα	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	7	5	35
Laptop (1-2)	Καταστροφή από σεισμό	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	7	4	28
Laptop (1-2)	Κλοπή	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	4	40
Printer (1-4)	Διακοπή ηλεκτρικού ρεύματος	Περιορισμός ορισμένων διαδικασιών	3	3	9
Printer (1-4)	Καταστροφή από φωτιά	Οικονομική επίπτωση. Περιορισμός ορισμένων διαδικασιών	6	3	18
Printer (1-4)	Καταστροφή από πλημύρα	Οικονομική επίπτωση. Περιορισμός ορισμένων διαδικασιών	6	3	18
Printer (1-4)	Καταστροφή από σεισμό	Οικονομική επίπτωση. Περιορισμός ορισμένων διαδικασιών	6	2	12
Printer (1-4)	Κλοπή	Οικονομική επίπτωση. Περιορισμός ορισμένων διαδικασιών	6	4	24
Backup NAS	Κακόβουλο λογισμικό	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	6	60
Backup NAS	Διακοπή ηλεκτρικού ρεύματος	Απώλεια διαθεσιμότητας των δεδομένων.	10	3	30
Backup NAS	Καταστροφή από φωτιά	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	10	3	30
Backup NAS	Καταστροφή από πλημύρα	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	10	3	30
Backup NAS	Καταστροφή από σεισμό	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	10	2	20
Backup NAS	Κλοπή	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	4	40
SVN Server	Κακόβουλο λογισμικό	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	6	60

SVN Server	Διακοπή ηλεκτρικού ρεύματος	Απώλεια διαθεσιμότητας των δεδομένων.	10	3	30
SVN Server	Καταστροφή από φωτιά	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	10	3	30
SVN Server	Καταστροφή από πλημύρα	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	10	3	30
SVN Server	Καταστροφή από σεισμό	Απώλεια διαθεσιμότητας, ακεραιότητας των δεδομένων.	10	2	20
SVN Server	Κλοπή	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	4	40
Test Host (1-3)	Κακόβουλο λογισμικό	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	4	2	8
Test Host (1-3)	Διακοπή ηλεκτρικού ρεύματος	Απώλεια διαθεσιμότητας των δεδομένων.	4	3	12
Test Host (1-3)	Καταστροφή από φωτιά	Οικονομική επίπτωση.	7	3	21
Test Host (1-3)	Καταστροφή από πλημύρα	Οικονομική επίπτωση.	7	3	21
Test Host (1-3)	Καταστροφή από σεισμό	Οικονομική επίπτωση.	7	2	14
Test Host (1-3)	Κλοπή	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων. Οικονομική επίπτωση.	10	4	40
Modem / Router / Firewall	Διακοπή ηλεκτρικού ρεύματος	Απώλεια διαθεσιμότητας των δεδομένων.	8	3	24
Modem / Router / Firewall	Καταστροφή από φωτιά	Απώλεια διαθεσιμότητας των δεδομένων. Οικονομική επίπτωση.	8	3	24
Modem / Router / Firewall	Καταστροφή από πλημύρα	Απώλεια διαθεσιμότητας των δεδομένων. Οικονομική επίπτωση.	8	3	24
Modem / Router / Firewall	Καταστροφή από σεισμό	Απώλεια διαθεσιμότητας των δεδομένων. Οικονομική επίπτωση.	8	2	16
Modem / Router / Firewall	Κλοπή	Απώλεια διαθεσιμότητας των δεδομένων. Οικονομική επίπτωση.	8	4	32
Router 2	Διακοπή ηλεκτρικού ρεύματος	Απώλεια διαθεσιμότητας των δεδομένων.	3	3	9
Router 2	Καταστροφή από φωτιά	Απώλεια διαθεσιμότητας των δεδομένων. Οικονομική επίπτωση.	4	3	12

Router 2	Καταστροφή από πλημύρα	Απώλεια διαθεσιμότητας των δεδομένων. Οικονομική επίπτωση.	4	3	12
Router 2	Καταστροφή από σεισμό	Απώλεια διαθεσιμότητας των δεδομένων. Οικονομική επίπτωση.	4	2	8
Router 2	Κλοπή	Απώλεια διαθεσιμότητας των δεδομένων. Οικονομική επίπτωση.	4	4	16
Workstation (1-8)	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Laptop (1-2)	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Backup NAS	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
SVN Server	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Modem / Router / Firewall	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Switch	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Test Host (1-3)	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Router 2	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Κτιριακές Εγκαταστάσεις/ Γραφεία	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	3	30
Συμβόλαια / NDAs	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	5	50
Συμβόλαια / NDAs	Καταστροφή από φωτιά	Απώλεια διαθεσιμότητας.	10	3	30
Συμβόλαια / NDAs	Καταστροφή από πλημύρα	Απώλεια διαθεσιμότητας.	10	3	30
Συμβόλαια / NDAs	Κλοπή	Απώλεια διαθεσιμότητας και εμπιστευτικότητας	10	6	60

		των δεδομένων, Νομικά ζητήματα.			
Mobile Agent Platform	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	3	30
Δικτυακές καλωδιώσεις	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	4	40
Κτιριακές Εγκαταστάσεις/ Γραφεία	Καταστροφή από φυσικά φαινόμενα	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	4	40
Μέσα αποθήκευσης ψηφιακών δεδομένων	Απόρριψη στα σκουπίδια/ανακύκλωση χωρίς να προηγηθεί η καταστροφή των δεδομένων	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	6	60
Έγγραφα	Απόρριψη στα σκουπίδια/ανακύκλωση χωρίς να προηγηθεί η καταστροφή των δεδομένων	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	6	60
Μέσα αποθήκευσης ψηφιακών δεδομένων	Υποκλοπή δεδομένων μέσα από την εταιρία	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	6	60
Πηγαίος Κώδικας	Υποκλοπή δεδομένων μέσα από την εταιρία	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	5	50
E-mails	Διαρροή πληροφοριών	Απώλεια εμπιστευτικότητας , Νομικά ζητήματα.	10	6	60
Έγγραφα	Διαρροή πληροφοριών	Απώλεια εμπιστευτικότητας , Νομικά ζητήματα.			0
Mobile Agents/Data	Διαρροή πληροφοριών	Απώλεια εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	10	6	60
Mobile Agents/Data	Κακόβουλοι agents	Απώλεια διαθεσιμότητας και ακεραιότητας των δεδομένων.	10	6	60
Production Hosts	Κακόβουλο λογισμικό	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων, Νομικά ζητήματα.	4	2	8
Production Hosts	Διακοπή ηλεκτρικού ρεύματος	Απώλεια διαθεσιμότητας των δεδομένων.	4	3	12
Production Hosts	Καταστροφή από φωτιά	Οικονομική επίπτωση.	7	3	21
Production Hosts	Καταστροφή από πλημύρα	Οικονομική επίπτωση.	7	3	21
Production Hosts	Καταστροφή από σεισμό	Οικονομική επίπτωση.	7	2	14

Production Hosts	Κλοπή	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων. Οικονομική επίπτωση.	10	4	40
Production Hosts	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Πολιτικές Ασφαλείας/Διαδικασίες/Σχεδιασμοί	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Αρχεία Καταγραφής (Αρχείο Καταγραφής)	Μη εξουσιοδοτημένη πρόσβαση	Απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων.	10	3	30
Πολιτικές Ασφαλείας/Διαδικασίες/Σχεδιασμοί	Διαρροή πληροφοριών	Απώλεια εμπιστευτικότητας των δεδομένων.	10	3	30
Αρχεία Καταγραφής (Αρχείο Καταγραφής)	Διαρροή πληροφοριών	Απώλεια εμπιστευτικότητας των δεδομένων.	10	3	30

Α.3 Αντιμετώπιση κινδύνων

Αντιμετώπιση Κινδύνων					
Περιουσιακό Στοιχείο	**Ευπάθεια**	**Έλεγχοι**	**Κίνδυνος**	**Αντιμετώπιση**	**Ημερομηνία Εφαρμογής Ελέγχων**
Διοίκηση	Μη καθιέρωση / κοινοποίηση της πολιτικής και των στόχων ασφάλειας.	Καθιέρωση / κοινοποίηση της πολιτικής και των στόχων ασφάλειας (5.2 Πολιτική.docx)	21	Μείωση Κινδύνου	01-05-19
Διοίκηση	Μη παροχή απαραίτητων πόρων για εφαρμογή του ΣΔΑΠ.	Γραπτή δέσμευση για παροχή απαραίτητων πόρων για υλοποίηση και εφαρμογή του ΣΔΑΠ (5.2 Πολιτική.docx)	45	Μείωση Κινδύνου	01-05-19
Διοίκηση	Μη τήρηση συμφωνιών/συμβολαίων	Γραπτή δέσμευση για τήρηση συμφωνιών/συμβολαίων	18	Μείωση Κινδύνου	01-05-19
Διοίκηση	Μη διενέργεια Ανασκόπησης Διοίκησης	Διενέργεια Ανασκόπησης Διοίκησης μια φορά τον χρόνο, συμφώνα με την παράγραφο 9.3 του προτύπου	16	Μείωση Κινδύνου	01-05-19
Διοίκηση	Ελλιπής ή μη καθορισμός ρόλων, ευθηνών και εξουσιών	Καθορισμός ρόλων, ευθηνών και εξουσιών	18	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Μη παρακολούθηση κίνησης δικτύου	Παρακολούθηση δικτύου για τυχόν απειλές μέσω IDS/IPS	45	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Μη παρακολούθηση του Antivirus	Παρακολούθηση Antivirus για τυχόν απειλές	30	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Λανθασμένη ρύθμιση του Firewall & Web Content Filter	Ρύθμιση firewall με τέτοιο τρόπο (κανόνες) ώστε να επιτρέπετε μόνο η αναγκαία εισερχόμενη/εξερχομένη κίνηση από και προς το δίκτυο του οργανισμού.	30	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Μη τήρηση αντιγράφων ασφάλειας	Τήρηση αντιγράφων ασφαλείας	40	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη ελέγχου χωρητικότητας	Διαχείριση χωρητικοτήτων	30	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη αναβάθμισης λογισμικού	Έλεγχος και αναβάθμιση του λογισμικού όλου του οργανισμού με τις τελευταίες ενημερώσεις ασφαλείας.	20	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη εφαρμογής ελέγχων πρόσβασης στα συστήματα	Δημιουργία πολιτικής για την εφαρμογή ελέγχου πρόσβασης στα συστήματα.	40	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Μη ανάλυση αρχείων καταγραφής (log files)	Τακτική ανασκόπηση αρχείων καταγραφής διαχειριστών και χειριστών	30	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη καταγραφής και αναφοράς	Καταγραφή και αναφορά	16	Μείωση Κινδύνου	01-05-19

	περιστατικών ασφάλειας	περιστατικών ασφαλείας.			
Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη αντιμετώπισης περιστατικών ασφάλειας	Αντιμετώπιση περιστατικών ασφαλείας. Τακτικός έλεγχος από τον διευθυντή ασφάλειας πληροφοριών και τον εσωτερικό ελεγκτή.	30	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Διακοπή ηλεκτρικού ρεύματος	Σύνδεση με UPS, η παροχή ηλεκτρικού ρεύματος στον οργανισμό γίνεται από δυο υπηρεσίες παροχής ηλεκτρικής ενέργειας	24	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Παράλειψη συντήρησης του εξοπλισμού	Συντήρηση εξοπλισμού ανά τακτά χρονικά διαστήματα	20	Μείωση Κινδύνου	01-05-19
Διαχειριστής Συστημάτων και Δικτύου	Απουσία λόγο ασθένειας	Προσωρινή λήψη καθηκόντων από άτομο του τμήματος των προγραμματιστών. Θα προηγηθεί σχετική εκπαίδευση.	54	Μείωση Κινδύνου	01-05-19
Προγραμματιστής	Παράλειψη ελέγχου της εφαρμογής, πριν την εκτέλεση της σε πραγματικές συνθήκες	Δημιουργία ενός περιβάλλοντος για τον έλεγχο των εφαρμογών πριν την εκτέλεση τους σε πραγματικές συνθήκες.	30	Μείωση Κινδύνου	01-05-19
Προγραμματιστής	Μη τήρηση εκδόσεων του πηγαίου κώδικα	Δημιουργία ενός συστήματος διαχείρισης του πηγαίου κώδικα (SVN Server)	32	Μείωση Κινδύνου	01-05-19
Προγραμματιστής	Μη εφαρμογή ελέγχων ασφαλείας κατά τον σχεδιασμό των εφαρμογών	Εφαρμογή ελέγχων ασφαλείας κατά τον σχεδιασμό των εφαρμογών	30	Μείωση Κινδύνου	01-05-19
Διευθυντής Ασφάλειας Πληροφοριών	Έλλειψη συντονισμού των δραστηριοτήτων που αφορούν το ΣΔΑΠ	Συντονισμός όλων των δραστηριοτήτων που αφορούν το ΣΔΑΠ, συμφώνα με τις απαιτήσεις του διεθνούς πρότυπου ISO 27001:2013	30	Μείωση Κινδύνου	01-05-19
Διευθυντής Ανθρώπινου Δυναμικού	Πρόσληψη ακατάλληλα καταρτισμένου προσωπικού	Καθορισμός κατάλληλων προσόντων/ εμπειρίας για κάθε θέση εργασίας	50	Μείωση Κινδύνου	01-05-19
Διευθυντής Ανθρώπινου Δυναμικού	Μη τήρηση διαδικασιών κατά την απόλυση προσωπικού	Καθορισμός σχετικής διαδικασίας. Άλλοι εμπλεκόμενοι είναι ο διαχειριστής συστημάτων και δικτύου και ο υπεύθυνος φυσικής ασφαλείας για την αφαίρεση των δικαιωμάτων πρόσβασης.	40	Μείωση Κινδύνου	01-05-19
Διευθυντής Ανθρώπινου Δυναμικού	Ελλιπής ή καθόλου εκπαίδευση / ευαισθητοποίησης του προσωπικού σε θέματα ασφάλειας δεδομένων	Τακτική εκπαίδευση/ενημέρωση του προσωπικού σε θέματα ασφάλειας πληροφοριών.	60	Μείωση Κινδύνου	01-05-19

Διευθυντής Ανθρώπινου Δυναμικού	Παράλειψη σύναψης συμφωνητικών εμπιστευτικότητας (NDAs) με προσωπικό, συνεργάτες / υπεργολάβους	Δημιουργία σχετικής διαδικασίας/πολιτικής που θα εφαρμόζεται κατά την πρόσληψη/ ανάθεσης έργου.	40	Μείωση Κινδύνου	01-05-19
Νομικός Σύμβουλος	Παράλειψη προσδιορισμού απαιτήσεων για την συμμόρφωση του οργανισμού με την νομοθεσία	Συμμόρφωση του οργανισμού με την νομοθεσία	20	Μείωση Κινδύνου	01-05-19
Υπεύθυνος Φυσικής Ασφάλειας	Μη υλοποίηση ελέγχων για κλοπή / βιομηχανικής κατασκοπείας.	Εγκατάσταση CCTV στο εσωτερικό και περιμετρικά του κτιρίου	50	Μείωση Κινδύνου	01-05-19
Υπεύθυνος Φυσικής Ασφάλειας	Μη υλοποίηση ελέγχων για φωτιά	Εγκατάσταση αντιπυρικού συστήματος, Εκπαίδευση προσωπικού, Ασκήσεις ετοιμότητας, επικοινωνία με τις αρχές.	60	Μείωση Κινδύνου	01-05-19
Υπεύθυνος Φυσικής Ασφάλειας	Μη υλοποίηση ελέγχων για πλημύρα	Εγκατάσταση αντιπλημμυρικού συστήματος, Εκπαίδευση προσωπικού, Ασκήσεις ετοιμότητας, επικοινωνία με τις αρχές.	40	Μείωση Κινδύνου	01-05-19
Υπεύθυνος Φυσικής Ασφάλειας	Μη υλοποίηση ελέγχων για Σεισμό	Εκπαίδευση προσωπικού, Ασκήσεις ετοιμότητας, επικοινωνία με τις αρχές.	24	Μείωση Κινδύνου	01-05-19
Συνεργείο Καθαρισμού	Κλοπή, Βιομηχανική κατασκοπεία	Υπογραφή σύμφωνου εμπιστευτικότητας, πολιτική καθαρού γραφείου, καθαρής οθόνης, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου, διαβάθμιση πληροφοριών	60	Μείωση Κινδύνου	01-05-19
Συνεργείο Καθαρισμού	Καταστροφή εξοπλισμού (από λάθος ή από πρόθεση)	Ενημέρωση σχετικά με την ευαισθησία του εξοπλισμού και του σωστού τρόπου καθαρισμού του.	50	Μείωση Κινδύνου	01-05-19
Εσωτερικός Ελεγκτής	Παράλειψη διενέργειας εσωτερικού ελέγχου	Διενέργεια εσωτερικού ελέγχου του ΣΔΑΠ κάθε 6 μήνες	30	Μείωση Κινδύνου	01-05-19
Workstation (1-8)	Κακόβουλο λογισμικό	Εγκατάσταση Antivirus, Antiransomware, εκπαίδευση του προσωπικού	60	Μείωση Κινδύνου	01-05-19
Workstation (1-8)	Διακοπή ηλεκτρικού ρεύματος	Σύνδεση με UPS, η παροχή ηλεκτρικού ρεύματος στον οργανισμό γίνεται από δυο υπηρεσίες παροχής ηλεκτρικής ενέργειας	15	Μείωση Κινδύνου	01-05-19
Workstation (1-8)	Καταστροφή από φωτιά	Εγκατάσταση αντιπυρικού συστήματος	21	Μείωση Κινδύνου	01-05-19

Workstation (1-8)	Καταστροφή από πλημύρα	Εγκατάσταση αντιπλημμυρικού συστήματος	21	Μείωση Κινδύνου	01-05-19
Workstation (1-8)	Καταστροφή από σεισμό	Προστασία εξοπλισμού από πτώση.	14	Μείωση Κινδύνου	01-05-19
Workstation (1-8)	Κλοπή	Χρήση fingerprint scanner για πρόσβαση στις εγκαταστάσεις, χρήση Smart Cards για πρόσβαση στα γραφεία, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου	40	Μείωση Κινδύνου	01-05-19
Laptop (1-2)	Κακόβουλο λογισμικό	Έλεγχοι ενάντια κακόβουλου λογισμικού σε συνδυασμό με σχετική εκπαίδευση του προσωπικού	60	Μείωση Κινδύνου	01-05-19
Laptop (1-2)	Διακοπή ηλεκτρικού ρεύματος	Σύνδεση με UPS, η παροχή ηλεκτρικού ρεύματος στον οργανισμό γίνεται από δυο υπηρεσίες παροχής ηλεκτρικής ενέργειας	5	Μείωση Κινδύνου	01-05-19
Laptop (1-2)	Καταστροφή από φωτιά	Εγκατάσταση αντιπυρικού συστήματος	35	Μείωση Κινδύνου	01-05-19
Laptop (1-2)	Καταστροφή από πλημύρα	Εγκατάσταση αντιπλημμυρικού συστήματος	35	Μείωση Κινδύνου	01-05-19
Laptop (1-2)	Καταστροφή από σεισμό	Προστασία εξοπλισμού από πτώση.	28	Μείωση Κινδύνου	01-05-19
Laptop (1-2)	Κλοπή	Χρήση fingerprint scanner για πρόσβαση στις εγκαταστάσεις, χρήση Smart Cards για πρόσβαση στα γραφεία, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου	40	Μείωση Κινδύνου	01-05-19
Printer (1-4)	Διακοπή ηλεκτρικού ρεύματος	Σύνδεση με UPS, η παροχή ηλεκτρικού ρεύματος στον οργανισμό γίνεται από δυο υπηρεσίες παροχής ηλεκτρικής ενέργειας	9	Μείωση Κινδύνου	01-05-19
Printer (1-4)	Καταστροφή από φωτιά	Εγκατάσταση αντιπυρικού συστήματος	18	Μείωση Κινδύνου	01-05-19
Printer (1-4)	Καταστροφή από πλημύρα	Εγκατάσταση αντιπλημμυρικού συστήματος	18	Μείωση Κινδύνου	01-05-19
Printer (1-4)	Καταστροφή από σεισμό	Προστασία εξοπλισμού από πτώση.	12	Μείωση Κινδύνου	01-05-19
Printer (1-4)	Κλοπή	Χρήση fingerprint scanner για πρόσβαση στις εγκαταστάσεις, χρήση Smart Cards για πρόσβαση στα γραφεία, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου	24	Μείωση Κινδύνου	01-05-19

Backup NAS	Κακόβουλο λογισμικό	Έλεγχοι ενάντια κακόβουλου λογισμικού σε συνδυασμό με σχετική εκπαίδευση του προσωπικού	60	Μείωση Κινδύνου	01-05-19
Backup NAS	Διακοπή ηλεκτρικού ρεύματος	Σύνδεση με UPS, η παροχή ηλεκτρικού ρεύματος στον οργανισμό γίνεται από δυο υπηρεσίες παροχής ηλεκτρικής ενέργειας	30	Μείωση Κινδύνου	01-05-19
Backup NAS	Καταστροφή από φωτιά	Εγκατάσταση αντιπυρικού συστήματος	30	Μείωση Κινδύνου	01-05-19
Backup NAS	Καταστροφή από πλημύρα	Εγκατάσταση αντιπλημμυρικού συστήματος	30	Μείωση Κινδύνου	01-05-19
Backup NAS	Καταστροφή από σεισμό	Προστασία εξοπλισμού από πτώση.	20	Μείωση Κινδύνου	01-05-19
Backup NAS	Κλοπή	Χρήση fingerprint scanner για πρόσβαση στις εγκαταστάσεις, χρήση Smart Cards για πρόσβαση στα γραφεία, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου	40	Μείωση Κινδύνου	01-05-19
SVN Server	Κακόβουλο λογισμικό	Έλεγχοι ενάντια κακόβουλου λογισμικού σε συνδυασμό με σχετική εκπαίδευση του προσωπικού	60	Μείωση Κινδύνου	01-05-19
SVN Server	Διακοπή ηλεκτρικού ρεύματος	Σύνδεση με UPS, η παροχή ηλεκτρικού ρεύματος στον οργανισμό γίνεται από δυο υπηρεσίες παροχής ηλεκτρικής ενέργειας	30	Μείωση Κινδύνου	01-05-19
SVN Server	Καταστροφή από φωτιά	Εγκατάσταση αντιπυρικού συστήματος	30	Μείωση Κινδύνου	01-05-19
SVN Server	Καταστροφή από πλημύρα	Εγκατάσταση αντιπλημμυρικού συστήματος	30	Μείωση Κινδύνου	01-05-19
SVN Server	Καταστροφή από σεισμό	Προστασία εξοπλισμού από πτώση.	20	Μείωση Κινδύνου	01-05-19
SVN Server	Κλοπή	Χρήση fingerprint scanner για πρόσβαση στις εγκαταστάσεις, χρήση Smart Cards για πρόσβαση στα γραφεία, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου	40	Μείωση Κινδύνου	01-05-19
Test Host (1-3)	Κακόβουλο λογισμικό	Έλεγχοι ενάντια κακόβουλου λογισμικού σε συνδυασμό με σχετική εκπαίδευση του προσωπικού	8	Μείωση Κινδύνου	01-05-19
Test Host (1-3)	Διακοπή ηλεκτρικού ρεύματος	Σύνδεση με UPS, η παροχή ηλεκτρικού ρεύματος στον οργανισμό γίνεται από δυο υπηρεσίες	12	Μείωση Κινδύνου	01-05-19

		παροχής ηλεκτρικής ενέργειας			
Test Host (1-3)	Καταστροφή από φωτιά	Εγκατάσταση αντιπυρικού συστήματος	21	Μείωση Κινδύνου	01-05-19
Test Host (1-3)	Καταστροφή από πλημύρα	Εγκατάσταση αντιπλημμυρικού συστήματος	21	Μείωση Κινδύνου	01-05-19
Test Host (1-3)	Καταστροφή από σεισμό	Προστασία εξοπλισμού από πτώση.	14	Μείωση Κινδύνου	01-05-19
Test Host (1-3)	Κλοπή	Χρήση Smart Cards για πρόσβαση στα γραφεία, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου	40	Μείωση Κινδύνου	01-05-19
Modem / Router / Firewall	Διακοπή ηλεκτρικού ρεύματος	Σύνδεση με UPS, η παροχή ηλεκτρικού ρεύματος στον οργανισμό γίνεται από δυο υπηρεσίες παροχής ηλεκτρικής ενέργειας	24	Μείωση Κινδύνου	01-05-19
Modem / Router / Firewall	Καταστροφή από φωτιά	Εγκατάσταση αντιπυρικού συστήματος	24	Μείωση Κινδύνου	01-05-19
Modem / Router / Firewall	Καταστροφή από πλημύρα	Εγκατάσταση αντιπλημμυρικού συστήματος	24	Μείωση Κινδύνου	01-05-19
Modem / Router / Firewall	Καταστροφή από σεισμό	Προστασία εξοπλισμού από πτώση.	16	Μείωση Κινδύνου	01-05-19
Modem / Router / Firewall	Κλοπή	Χρήση fingerprint scanner για πρόσβαση στις εγκαταστάσεις, χρήση Smart Cards για πρόσβαση στα γραφεία, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου	32	Μείωση Κινδύνου	01-05-19
Router 2	Διακοπή ηλεκτρικού ρεύματος	Σύνδεση με UPS, η παροχή ηλεκτρικού ρεύματος στον οργανισμό γίνεται από δυο υπηρεσίες παροχής ηλεκτρικής ενέργειας	9	Μείωση Κινδύνου	01-05-19
Router 2	Καταστροφή από φωτιά	Εγκατάσταση αντιπυρικού συστήματος	12	Μείωση Κινδύνου	01-05-19
Router 2	Καταστροφή από πλημύρα	Εγκατάσταση αντιπλημμυρικού συστήματος	12	Μείωση Κινδύνου	01-05-19
Router 2	Καταστροφή από σεισμό	Προστασία εξοπλισμού από πτώση.	8	Μείωση Κινδύνου	01-05-19
Router 2	Κλοπή	Χρήση fingerprint scanner για πρόσβαση στις εγκαταστάσεις, χρήση Smart Cards για πρόσβαση στα γραφεία, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου	16	Μείωση Κινδύνου	01-05-19

Workstation (1-8)	Μη εξουσιοδοτημένη πρόσβαση	Χρήση δυνατού κωδικού πρόσβασης, Κρυπτογράφηση σκληρού δίσκου, Πολιτική καθαρού γραφείου και καθαρής οθόνης, Καταγραφή συμβάντων, Προστασία καταγραφών συμβάντων, Έλεγχος εγκατάστασης λογισμικού, Περιορισμός εγκατάστασης λογισμικού, Ενημερώσεις λογισμικού	30	Μείωση Κινδύνου	01-05-19
Laptop (1-2)	Μη εξουσιοδοτημένη πρόσβαση	Χρήση δυνατού κωδικού πρόσβασης, Κρυπτογράφηση σκληρού δίσκου, Πολιτική καθαρού γραφείου και καθαρής οθόνης, Καταγραφή συμβάντων, Προστασία καταγραφών συμβάντων, Έλεγχος εγκατάστασης λογισμικού, Περιορισμός εγκατάστασης λογισμικού, Σύνδεση στο διαδίκτυο μέσω VPN	30	Μείωση Κινδύνου	01-05-19
Backup NAS	Μη εξουσιοδοτημένη πρόσβαση	Χρήση δυνατού κωδικού πρόσβασης, Κρυπτογράφηση σκληρού δίσκου, Πολιτική καθαρού γραφείου και καθαρής οθόνης, Καταγραφή συμβάντων, Προστασία καταγραφών συμβάντων, Έλεγχος εγκατάστασης λογισμικού, Περιορισμός εγκατάστασης λογισμικού, Ενημερώσεις λογισμικού	30	Μείωση Κινδύνου	01-05-19
SVN Server	Μη εξουσιοδοτημένη πρόσβαση	Χρήση δυνατού κωδικού πρόσβασης, Κρυπτογράφηση σκληρού δίσκου, Πολιτική καθαρού γραφείου και καθαρής οθόνης, Καταγραφή συμβάντων, Προστασία καταγραφών συμβάντων, Έλεγχος εγκατάστασης λογισμικού, Περιορισμός εγκατάστασης λογισμικού, Ενημερώσεις λογισμικού	30	Μείωση Κινδύνου	01-05-19

Modem / Router / Firewall	Μη εξουσιοδοτημένη πρόσβαση	Χρήση δυνατού κωδικού πρόσβασης, Καταγραφή συμβάντων, Προστασία καταγραφών συμβάντων	30	Μείωση Κινδύνου	01-05-19
Switch	Μη εξουσιοδοτημένη πρόσβαση	Χρήση δυνατού κωδικού πρόσβασης, Καταγραφή συμβάντων, Προστασία καταγραφών συμβάντων	30	Μείωση Κινδύνου	01-05-19
Test Host (1-3)	Μη εξουσιοδοτημένη πρόσβαση	Χρήση δυνατού κωδικού πρόσβασης, Κρυπτογράφηση σκληρού δίσκου, Πολιτική καθαρού γραφείου και καθαρής οθόνης, Καταγραφή συμβάντων, Προστασία καταγραφών συμβάντων, Έλεγχος εγκατάστασης λογισμικού, Περιορισμός εγκατάστασης λογισμικού, Ενημερώσεις λογισμικού	30	Μείωση Κινδύνου	01-05-19
Router 2	Μη εξουσιοδοτημένη πρόσβαση	Χρήση δυνατού κωδικού πρόσβασης, Καταγραφή συμβάντων, Προστασία καταγραφών συμβάντων	30	Μείωση Κινδύνου	01-05-19
Κτιριακές Εγκαταστάσεις/ Γραφεία	Μη εξουσιοδοτημένη πρόσβαση	Εγκατάσταση CCTV περιμετρικά, Χρήση Smart Cards για πρόσβαση στα γραφεία, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου	30	Μείωση Κινδύνου	01-05-19
Συμβόλαια / NDAs	Μη εξουσιοδοτημένη πρόσβαση	Πολιτική καθαρού γραφείου και καθαρής οθόνης, Αποθήκευση στον αποθηκευτικός χώρο εγγράφων μετά την χρήση τους.	50	Μείωση Κινδύνου	01-05-19
Συμβόλαια / NDAs	Καταστροφή από φωτιά	Εγκατάσταση αντιπυρικού συστήματος	30	Μείωση Κινδύνου	01-05-19
Συμβόλαια / NDAs	Καταστροφή από πλημύρα	Εγκατάσταση αντιπλημμυρικού συστήματος	30	Μείωση Κινδύνου	01-05-19
Συμβόλαια / NDAs	Κλοπή	Αποθήκευση στον αποθηκευτικός χώρο εγγράφων μετά την χρήση τους, διαβάθμιση πληροφοριών, πολιτική καθαρού γραφείου καθαρής οθόνης, Χρήση fingerprint scanner για πρόσβαση στις εγκαταστάσεις, χρήση Smart Cards για πρόσβαση στα	60	Μείωση Κινδύνου	01-05-19

		γραφεία, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου			
Mobile Agent Platform	Μη εξουσιοδοτημένη πρόσβαση	Ενεργοποίηση καταγραφής συμβάντων, Προστασία των αρχείων καταγραφών συμβάντων, αλλαγή προκαθορισμένων κωδικών πρόσβασης, προστασία αρχείου ρυθμίσεων, αφαίρεση ευαίσθητων δεδομένων (π.χ. κωδικών) από το αρχείο ρυθμίσεων, χρήση δυνατών κωδικών πρόσβασης	30	Μείωση Κινδύνου	01-05-19
Δικτυακές καλωδιώσεις	Μη εξουσιοδοτημένη πρόσβαση	Προστασία καλωδιώσεων	40	Μείωση Κινδύνου	01-05-19
Κτιριακές Εγκαταστάσεις/ Γραφεία	Καταστροφή από φυσικά φαινόμενα	Εγκατάσταση αντιπλημμυρικού και αντιπυρικού συστήματος, Προστασία εξοπλισμού από πτώση.	40	Μείωση Κινδύνου	01-05-19
Μέσα αποθήκευσης ψηφιακών δεδομένων	Απόρριψη στα σκουπίδια/ανακύκλωση χωρίς να προηγηθεί η καταστροφή των δεδομένων	Διαγραφή δεδομένων ή/και Καταστροφή του μέσου με τον καταστροφέα μέσων αποθήκευσης	60	Μείωση Κινδύνου	01-05-19
Έγγραφα	Απόρριψη στα σκουπίδια/ανακύκλωση χωρίς να προηγηθεί η καταστροφή των δεδομένων	Καταστροφή του μέσου με τον καταστροφέα εγγράφων	60	Μείωση Κινδύνου	01-05-19
Μέσα αποθήκευσης ψηφιακών δεδομένων	Υποκλοπή δεδομένων μέσα από την εταιρία	Υπογραφή NDA από όλο το προσωπικό του οργανισμού, Απενεργοποίηση USB port/CD/DVD writer, απαγόρευση λήψης φωτογραφιών	60	Μείωση Κινδύνου	01-05-19
Πηγαίος Κώδικας	Υποκλοπή δεδομένων μέσα από την εταιρία	Υπογραφή NDA από όλο το προσωπικό του οργανισμού, παρακολούθηση δικτύου, παρακολούθηση επισκεψιμότητας ύποπτων σελίδων (π.χ. file sharing) από το προσωπικό, απαγόρευση λήψης φωτογραφιών, διαβάθμιση πληροφοριών.	50	Μείωση Κινδύνου	01-05-19
E-mails	Διαρροή πληροφοριών	Χρήση Κρυπτογράφησης	60	Μείωση Κινδύνου	01-05-19
Έγγραφα	Διαρροή πληροφοριών	Χρήση της βαλίτσας ασφαλείας για την μεταφορά Εγγράφων	0	Μείωση Κινδύνου	01-05-19

Mobile Agents/Data	Διαρροή πληροφοριών	Χρήση Κρυπτογράφησης στα δεδομένα που μεταφέρει ο agent αλλά και στο κανάλι επικοινωνίας (χρήση SSL)	60	Μείωση Κινδύνου	01-05-19
Mobile Agents/Data	Κακόβουλοι agents	**Οργανωτικοί:** Εφαρμογή συστήματος βαθμολόγησης πρακτορείων, Αποδοχή agents μόνο από πρακτορεία καλής φήμης, Σύναψη συμβολαίων μεταξύ πρακτορείων όπου θα απαγορεύει κακόβουλες ενέργειες μεταξύ πρακτορείων (συμφωνία προθέσεων), Κατάθεση Αίτησης με τα στοιχεία του mobile agent και την διαδρομή που θα ακολουθήσει, Τακτικές αμοιβαίες επιθεωρήσεις (π.χ. του κώδικα ή του ISMS) μεταξύ πρακτορείων (2nd ή 3rd Party Audits **Τεχνικοί:** Εκτέλεση του agent σε ασφαλές περιβάλλον (sandbox), Περιορισμός agents σε πόρους του συστήματος (CPU, RAM, Network, Files, κτλ.), Λήψη εξουσιοδότηση για εκτέλεση κώδικα στον Host, Αυθεντικοποίηση Agent/Host, Έλεγχος ακεραιότητας δεδομένων, Μηχανισμοί μη αποκήρυξης αποστολής/ λήψης/ εκτέλεσης των agents	60	Μείωση Κινδύνου	01-05-19
Production Hosts	Κακόβουλο λογισμικό	Έλεγχοι ενάντια κακόβουλου λογισμικού σε συνδυασμό με σχετική εκπαίδευση του προσωπικού	8	Μείωση Κινδύνου	01-05-19
Production Hosts	Διακοπή ηλεκτρικού ρεύματος	Σύνδεση με UPS, η παροχή ηλεκτρικού ρεύματος στον οργανισμό γίνεται από δυο υπηρεσίες παροχής ηλεκτρικής ενέργειας	12	Μείωση Κινδύνου	01-05-19
Production Hosts	Καταστροφή από φωτιά	Εγκατάσταση αντιπυρικού συστήματος	21	Μείωση Κινδύνου	01-05-19
Production Hosts	Καταστροφή από πλημύρα	Εγκατάσταση αντιπλημμυρικού συστήματος	21	Μείωση Κινδύνου	01-05-19
Production Hosts	Καταστροφή από σεισμό	Προστασία εξοπλισμού από πτώση.	14	Μείωση Κινδύνου	01-05-19

Production Hosts	Κλοπή	Χρήση fingerprint scanner για πρόσβαση στις εγκαταστάσεις, χρήση Smart Cards για πρόσβαση στα γραφεία, Εγκατάσταση CCTV στο εσωτερικό του κτιρίου	40	Μείωση Κινδύνου	01-05-19
Production Hosts	Μη εξουσιοδοτημένη πρόσβαση	Χρήση δυνατού κωδικού πρόσβασης, Κρυπτογράφηση σκληρού δίσκου, Πολιτική καθαρού γραφείου και καθαρής οθόνης, Καταγραφή συμβάντων, Προστασία καταγραφών συμβάντων, Έλεγχος εγκατάστασης λογισμικού, Περιορισμός εγκατάστασης λογισμικού, write blockers στις θύρες USB, Ενημερώσεις λογισμικού	30	Μείωση Κινδύνου	01-05-19
Πολιτικές Ασφαλείας/Διαδικασίες/Σχεδιασμοί	Μη εξουσιοδοτημένη πρόσβαση	Κρυπτογράφηση σκληρού δίσκου, Πολιτική καθαρού γραφείου και καθαρής οθόνης, Καταγραφή συμβάντων	30	Μείωση Κινδύνου	01-05-19
Αρχεια Καταγραφής (Αρχείο Καταγραφήςs)	Μη εξουσιοδοτημένη πρόσβαση	Κρυπτογράφηση σκληρού δίσκου, Πολιτική καθαρού γραφείου και καθαρής οθόνης, Καταγραφή συμβάντων	30	Μείωση Κινδύνου	01-05-19
Πολιτικές Ασφαλείας/Διαδικασίες/Σχεδιασμοί	Διαρροή πληροφοριών	Υπογραφή NDA από όλο το προσωπικό του οργανισμού	30	Μείωση Κινδύνου	01-05-19
Αρχεια Καταγραφής (Αρχείο Καταγραφήςs)	Διαρροή πληροφοριών	Υπογραφή NDA από όλο το προσωπικό του οργανισμού	30	Μείωση Κινδύνου	01-05-19

Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Παράρτημα Β

Πολιτικές και Διαδικασίες Ασφαλείας

Β.1 Πολιτικές Ασφαλείας

Πολιτική 001: Επικοινωνία με τις αρχές και με ομάδες ειδικών ενδιαφερόντων

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι:

- Θα υπάρξει επικοινωνία με τις αρχές σε περίπτωση περιστατικού ασφαλείας.
- Θα υπάρξει επικοινωνία με ομάδες ειδικών ενδιαφερόντων σε περίπτωση περιστατικού ασφαλείας για την λήψη συμβουλευτικών υπηρεσιών.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η επικοινωνία με τις Αρχές και με Ομάδες ειδικών ενδιαφερόντων, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013 και τον Γενικό Κανονισμό της Ε.Ε για την Προστασία Δεδομένων προσωπικού χαρακτήρα (GDPR).

Έλεγχοι από το Παράρτημα Α: Α.6.1.3, Α.6.1.4

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από τους:

- Διευθυντή Ασφάλειας Πληροφοριών
- Διευθυντή Διαχείρισης Εγκαταστάσεων

4. Πολιτική

- Επικοινωνία με τις αρχές

Σε περίπτωση περιστατικού ασφαλείας πρέπει να γίνει επικοινωνία με τις παρακάτω υπεύθυνες αρχές. Μετά την επικοινωνία πρέπει να συμπληρωθεί το αρχείο καταγραφής 008.

Περιστατικό	Υπεύθυνη Αρχή	Τηλέφωνο/E-mail	Υπεύθυνος Επικοινωνίας
Κλοπή	Αστυνομία	122	Διευθυντής Διαχείρισης Εγκαταστάσεων
Φωτιά	Πυροσβεστική	122	Διευθυντής Διαχείρισης Εγκαταστάσεων
Πλημύρα	Πυροσβεστική	122	Διευθυντής Διαχείρισης Εγκαταστάσεων
Περιστατικό Υγείας	Ασθενοφόρο	122	Διευθυντής Διαχείρισης Εγκαταστάσεων
Σεισμός	Πυροσβεστική	122	Διευθυντής Διαχείρισης Εγκαταστάσεων

Διαρροή Προσωπικών Δεδομένων	Γραφείο επιτρόπου προστασίας δεδομένων προσωπικού χαρακτήρα	+357-22818456 commissioner@dataprotection.gov.cy Αποστολή έντυπου γνωστοποίησης περιστατικών παραβίασης	Διευθυντής Ασφάλειας Πληροφοριών
Κυβερνοεπίθεση	Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος	Φόρμα Καταχώρησης Καταγγελιών/Πληροφοριών για θέματα ηλεκτρονικού εγκλήματος - https://goo.gl/XncZEt	Διευθυντής Ασφάλειας Πληροφοριών

- Επικοινωνία με ομάδες ειδικών ενδιαφερόντων

Ενδιαφέροντα	Ομάδες ειδικών ενδιαφερόντων
Ασφάλεια δεδομένων	ISF - https://www.securityforum.org/ IFSEC global - https://www.ifsecglobal.com/ IT Governance - https://www.itgovernance.co.uk/ Advisera (ISO 27001 Academy) - https://advisera.com/27001academy/ SANS Institute - https://www.sans.org/
Mobile Agents	Aglets Mailing List - https://sourceforge.net/p/aglets/mailman/ Academic Research Papers - https://www.springer.com/gp
Φυσική Ασφάλεια	IFSEC global - https://www.ifsecglobal.com/

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 002: Ασφάλεια πληροφοριών στην διαχείριση έργων

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θέματα που αφορούν την ασφάλεια πληροφοριών θα αντιμετωπίζονται καθ' όλη την διάρκεια ανάπτυξης και διαχείρισης των έργων του οργανισμού.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η αντιμετώπιση θεμάτων που αφορούν την ασφάλεια πληροφοριών καθ' όλη την διάρκεια ανάπτυξης και διαχείρισης των έργων του οργανισμού, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013 και τον Γενικό Κανονισμό της Ε.Ε για την Προστασία Δεδομένων προσωπικού χαρακτήρα (GDPR).

Έλεγχοι από το Παράρτημα Α: Α.6.1.5

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από όλους τους υπαλλήλους που συμμετέχουν στον σχεδιασμό, υλοποίηση και διαχείριση έργων, ανεξαρτήτως τύπου.

4. Πολιτική

Θέματα που αφορούν την ασφάλεια πληροφοριών θα πρέπει να αντιμετωπίζονται κατά την διάρκεια του σχεδιασμού (απαιτήσεις ασφαλείας), υλοποίησης και διαχείρισης όλων έργων του οργανισμού, ανεξαρτήτως τύπου.

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 003: Ασφάλεια κινητών συσκευών

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θα λαμβάνονται επαρκή μέτρα ασφαλείας σε κινητές συσκευές που θα λειτουργούν εκτός του οργανισμού.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η λήψη επαρκών μέτρων ασφάλειας σε κινητές συσκευές, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013 και τον Γενικό Κανονισμό της Ε.Ε για την Προστασία Δεδομένων προσωπικού χαρακτήρα (GDPR).

Έλεγχοι από το Παράρτημα Α: Α.6.2.1, Α.6.2.2

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από τους:

- Διοίκηση (Περιουσιακό στοιχείο: Laptop 2)
- Εσωτερικό Ελεγκτή (Περιουσιακό στοιχείο: Laptop 1)

4. Πολιτική

Όλες οι κινητές συσκευές που θα λειτουργούν εκτός του οργανισμού θα πρέπει:

- Να έχουν ενεργοποιημένη την κρυπτογράφηση σε όλα τα μέσα αποθήκευσης.
- Όταν είναι αναγκαίο να συνδεθούν στο διαδίκτυο, αυτό να γίνεται μέσω ασφαλών καναλιών (Τεχνολογία VPN) και επιβεβαιώνοντας το όνομα του δικτύου (SSID) με τον εκάστοτε υπεύθυνο.
- Απαγορεύεται η σύνδεση σε δημόσια σημεία εισόδου στο διαδίκτυο (Public Access Points).
- Η αποστολή /λήψη e-mail να γίνεται όποτε είναι αναγκαίο και με την χρήση κρυπτογράφησης.
- Χρήση δυνατών κωδικών πρόσβασης.
- Ενεργοποίηση Screen Saver με κλείδωμα οθόνης μετά από 1 λεπτό.
- Να είναι σε συνεχή επιτήρηση από τον χρήστη του.
- Να επιστρέφεται αμέσως μετά την χρήση του στις εγκαταστάσεις του οργανισμού.

Απαγορεύεται η εργασία εξ ’αποστάσεως (Teleworking).

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 004: Ασφάλεια ανθρώπινου δυναμικού

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θα λαμβάνονται επαρκή μέτρα ασφαλείας πριν, κατά την διάρκεια και μετά τον τερματισμό απασχόλησης του προσωπικού.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η λήψη επαρκών μέτρων ασφάλειας που αφορά το ανθρώπινο δυναμικό, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από τους:

- Διευθυντή Ανθρώπινου Δυναμικού

4. Πολιτική

Πριν την πρόσληψη θα πρέπει να γίνει:

- Έλεγχος επαγγελματικής επάρκειας του υποψηφίου.
- Επικοινωνία με προηγουμένους εργοδότες για λήψη πληροφοριών σχετικά:
    - Με τον χαρακτήρα, το ήθος και τον επαγγελματισμό του υποψηφίου.
    - Τυχών πειθαρχικά παραπτώματα.
    - Τους λόγους αποχώρησης.
- Λήψη αντιγράφων τίτλων σπουδών/εκπαίδευσης και ενημέρωση του σχετικού αρχείου (Αρχείο Καταγραφής 006)
- Επικοινωνία με τα εκπαιδευτικά ιδρύματα που φοίτησε ο υποψήφιος για λήψη πληροφοριών σχετικά με την εγκυρότητα των τίτλων σπουδών/εκπαίδευσης.
- Παρουσίαση βεβαίωσης λευκού ποινικού μητρώου.
- Υπογραφή συμβολαίων που αφορούν τους όρους και τις συνθήκες εργασίας
- Υπογραφή συμφωνητικού εμπιστευτικότητας (NDA)

Μετά την πρόσληψη θα πρέπει να γίνει:

- Δυνατότητα πρόσβασης στις κτιριακές εγκαταστάσεις και στα συστήματα του οργανισμού ανάλογα με τα καθήκοντα του προσωπικού.
- Ενημέρωση/Εκπαίδευση του προσωπικού σχετικά με τις πολιτικές ασφάλειας, διαδικασίες ή άλλη εκπαίδευση που πρέπει να εφαρμόζει κατά την εκτέλεση των καθηκόντων του και ενημέρωση του σχετικού αρχείου (Αρχείο Καταγραφής 007).
- Τακτική επικοινωνία με το προσωπικό για θέματα που αφορούν την εκπαίδευση τους.

Κατά τον τερματισμό της απασχόλησης θα πρέπει να γίνει:

- Ενημέρωση σχετικά με τα καθήκοντα που αφορούν την ασφάλεια πληροφοριών που παραμένουν ενεργά μετά τον τερματισμό απασχόλησης ή αλλαγής εργοδότη (π.χ. NDAs).

- Επιστροφή όλων των περιουσιακών στοιχείων του οργανισμού που έχουν στην κατοχή τους.
- Αφαίρεση δικαιωμάτων πρόσβασης στις κτιριακές εγκαταστάσεις και στα συστήματα του οργανισμού. Αυτό πρέπει να γίνεται σε συντονισμό με τους:

    - Διευθυντή Ασφάλειας Πληροφοριών
    - Διαχειριστή Συστημάτων και Δικτύου
    - Υπεύθυνο Φυσικής Ασφάλειας

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 005: Διαβάθμιση των πληροφοριών

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι όλες οι πληροφορίες του οργανισμού θα είναι διαβαθμισμένες.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η επισήμανση της σημαντικότητας της πληροφορίας ώστε να φαίνεται η ανάγκη και η προτεραιότητα της προστασίας που χρειάζεται, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.8.2.1, Α.8.2.2

3. Πεδίο Εφαρμογής

Ο καθορισμός του επιπέδου διαβάθμισης για το κάθε περιουσιακό στοιχείο καθορίζεται από τον Διευθυντής Ασφάλειας Πληροφοριών (Αρχείο Καταγραφής 003), ενώ η πολιτική εφαρμόζεται από ιδιοκτήτες της εκάστοτε πληροφορίας.

4. Πολιτική

Οι πληροφορίες πρέπει να διαβαθμίζονται ως εξής:

- **Απόρρητο** – Σε πληροφορίες που αν αποκαλυφθούν σε μη εξουσιοδοτημένο άτομο, είναι δυνατό να προκαλέσει τεράστια ζημιά στον οργανισμό.
- **Εμπιστευτικό** – Σε πληροφορίες που αν αποκαλυφθούν σε μη εξουσιοδοτημένο άτομο, είναι δυνατό να προκαλέσει μεγάλη ζημιά στον οργανισμό.
- **Περιορισμένης Χρήσης** – Σε πληροφορίες που αν αποκαλυφθούν σε μη εξουσιοδοτημένο άτομο, είναι δυνατό να προκαλέσει αρνητικές επιπτώσεις στον οργανισμό.
- **Εσωτερικής Χρήσης** – Σε πληροφορίες που αν αποκαλυφθούν σε μη εξουσιοδοτημένο άτομο, είναι δυνατό να προκαλέσει μικρή ζημιά στον οργανισμό.
- **Δημόσιο** – Σε πληροφορίες που αν αποκαλυφθούν σε μη εξουσιοδοτημένο άτομο, δεν θα προκαλέσει καμία ζημιά στον οργανισμό.

Η διαβάθμιση της πληροφορίας πρέπει να γίνεται από τον ιδιοκτήτη της εκάστοτε πληροφορίας στο πάνω αριστερό μέρος του εγγράφου/E-mail/μέσου αποθήκευσης με χρώμα κόκκινο.
Στην περίπτωση πηγαίου κώδικα η διαβάθμιση πρέπει να αναγράφεται στην αρχή του κειμένου (μέσα σε σχόλια).
Στην περίπτωση αποστολής εγγράφου/E-mail με διαβάθμιση «ΑΠΟΡΡΙΤΟ» ή «ΕΜΠΙΣΤΕΥΤΙΚΟ» στο κάτω μέρος πρέπει να αναγράφετε η παρακάτω ειδοποίηση εμπιστευτικότητας:

«*ΕΙΔΟΠΟΙΗΣΗ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ:*

Τα περιεχόμενα αυτού του μνήματος και όλων των συνημμένων απευθύνονται μόνο στον παραλήπτη (ή παραλήπτες) και ενδέχεται να περιέχουν απόρρητες ή/και εμπιστευτικές πληροφορίες. Σε περίπτωση που δεν είστε εσείς ο σκοπούμενος παραλήπτης παρακαλούμε όπως ειδοποιήσετε τον αποστολέα και στην συνέχεια διαγράψτε/καταστρέψτε το μνήμα και όλα τα συνημμένα. Η αντιγραφή, χρήση η κοινοποίηση σε τρίτους, αντίκειται στον περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας Νόμου»

Επίσης, η διαβάθμιση πρέπει να αναφέρεται λεκτικά, σε περίπτωση που η πληροφορία μεταδίδεται προφορικά.

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 006: Αποδεκτή χρήση των περιουσιακών στοιχείων

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι όλα τα περιουσιακά στοιχεία και οι πληροφορίες του οργανισμού θα χειρίζονται με αποδεκτό τρόπο από όλο το προσωπικό.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η αποδεκτή χρήση των περιουσιακών στοιχείων του οργανισμού, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.8.1.3

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από ιδιοκτήτες περιουσιακών στοιχείων του οργανισμού.

4. Πολιτική

Τα περιουσιακά στοιχεία του οργανισμού πρέπει να χρησιμοποιούνται μόνο από τους ιδιοκτήτες τους και με τέτοιο τρόπο ώστε:

- Να εκτελούν μόνο εργασίες που σχετίζονται με τις δραστηριότητες του οργανισμού.
- Να γίνεται σύμφωνα με την εκπαίδευση ή τις επίσημες οδηγίες (User Manual) χρήσης του κατασκευαστή (στην περίπτωση υλικού/εξοπλισμού).
- Να γίνεται σύμφωνα με την επίσημη τεκμηρίωση (Documentation) του κατασκευαστή (στην περίπτωση λογισμικού).
- Να διασφαλίζεται η ασφάλεια τους σύμφωνα με τις πολιτικές (Policies) ασφάλειας του οργανισμού.

Απαγορεύεται η χρήση περιουσιακών στοιχείων που δεν ανήκουν στον οργανισμό (π.χ. USB Flash Drives).

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 007: Συμμόρφωση με τις απαιτήσεις της νομοθεσίας και των συμβολαίων

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι όλο το προσωπικό συμμορφώνεται με τις απαιτήσεις της νομοθεσίας, των συμβολαίων και των πνευματικών δικαιωμάτων.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι ο καθορισμός και ή καταγραφή των απαιτήσεων της νομοθεσίας, των συμβολαίων και των πνευματικών δικαιωμάτων που πρέπει να συμμορφώνεται ο οργανισμός, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.13.2.4, Α.18.1.1, Α.18.1.2, Α.18.1.4, Α.18.1.5

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από τον Νομικό Σύμβουλο του οργανισμού.

4. Πολιτική

Ο οργανισμός πρέπει να συμμορφώνεται με τους παρακάτω νόμους, οδηγίες, συμβόλαια, πνευματικά δικαιώματα και άλλες απαιτήσεις του οργανισμού:

Νόμοι/Οδηγίες:

1. Ο περί της Σύμβασης κατά του Εγκλήματος μέσω του Διαδικτύου Νόμος του 2004
2. Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας Νόμος
3. Οδηγία Για την Επεξεργασία Προσωπικών Δεδομένων Στον Τομέα των Εργασιακών Σχέσεων
4. Οδηγία για την ΒΙΝΤΕΟ – ΠΑΡΑΚΟΛΟΥΘΗΣΗ
5. Γενικός Κανονισμός της Ε.Ε για την Προστασία Δεδομένων (GDPR)
6. Ο περί Συμβάσεων Νόμος (ΚΕΦ.149)
7. Ο περί του Δικαιώματος Πνευματικής Ιδιοκτησίας και Συγγενικών Δικαιωμάτων Νόμος του 2017
8. Οδηγία 2009/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Απριλίου 2009 , για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών
9. Εργατική Νομοθεσία:
    - Νόμοι/Κανονισμοί/Διατάγματα: http://www.mlsi.gov.cy/mlsi/dlr/dlr.nsf/page17_gr/page17_gr
    - Οδηγοί και άλλο πληροφοριακό υλικό: http://www.mlsi.gov.cy/mlsi/dlr/dlr.nsf/page18_gr/page18_gr?OpenDocument

Συμβόλαια:

Πρέπει να υπογράφονται τα παρακάτω:

1. Συμβόλαιο εργοδότη – εργαζομένου (Συμβόλαιο 001)

2. Συμβόλαια μεταξύ πρακτορείων όπου θα απαγορεύει κακόβουλες ενέργειες μεταξύ πρακτορείων και που θα καθορίζει κανόνες στην χρήση κρυπτογραφικών ελέγχων (Συμβόλαιο 002).
3. Υπογραφή συμφώνων εμπιστευτικότητας από όλο το προσωπικό και τους εξωτερικούς συνεργάτες (NDA 001)

Πνευματικά δικαιώματα:

1. Όλο το ιδιόκτητο λογισμικό που χρησιμοποιεί ο οργανισμός πρέπει να έχει γνήσιες άδειες χρήσης.

Άλλες απαιτήσεις:

1. Όλα τα αρχεία καταγραφών που αφορούν το ΣΔΑΠ, πρέπει να προστατεύονται κατάλληλα από απώλεια, παραποίηση, μη εξουσιοδοτημένη πρόσβαση και μη εξουσιοδότηση κοινοποίηση σε τρίτους.

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 008: Απαιτήσεις του οργανισμού για τον έλεγχο πρόσβασης

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θα καθιερωθούν κανόνες ελέγχου πρόσβασης στα συστήματα και εγκαταστάσεις του οργανισμού.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι ο καθορισμός κανόνων ελέγχου πρόσβασης στα συστήματα και εγκαταστάσεις του οργανισμού, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.9.1.1, Α.9.1.2, Α.9.2.3, Α.9.2.4, Α.9.2.5, Α.9.4.1

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από τους:

- Διαχειριστή Συστημάτων και Δικτύου και
- Υπεύθυνο Φυσικής Ασφάλειας

4. Πολιτική

Προφίλ χρηστών

Προφίλ	Πρόσβαση σε συστήματα	Φυσική Πρόσβαση σε εγκαταστάσεις
Α	• Πρόσβαση στο διαδίκτυο • Δίκτυο, Εφαρμογές και συστήματα του τμήματος	• Γραφείο τμήματος
Β	• Προφίλ Α • Δίκτυο, Εφαρμογές και συστήματα όλων των υπολοίπων τμημάτων	• Γραφεία όλων των τμημάτων
Γ	• Προφίλ Α	• Γραφεία όλων των τμημάτων • Αποθηκευτικός Χώρος Εγγράφων & Μέσων Αποθήκευσης
Δ	• Προφίλ Α	• Γραφεία όλων τμημάτων
Ε	-	• Γραφεία όλων των τμημάτων (*) • Αποθηκευτικός Χώρος Εγγράφων & Μέσων Αποθήκευσης (*)
Ζ	-	• Γραφεία όλων των τμημάτων (*)
Η	• Κώδικας	-

* Καταγραφή στο βιβλίο επισκεπτών, Ζωντανή παρακολούθηση κινήσεων από τον υπεύθυνο φυσικής ασφάλειας μέσω CCTV ή με την συνοδεία του υπεύθυνου φυσικής ασφάλειας.

Δικαιώματα πρόφασης στα συστήματα και τις φυσικές εγκαταστάσεις του οργανισμού:

Ρόλος	Προφίλ
Διοίκηση	Α, Β, Γ
Διευθυντής Πληροφορικής	Β, Η
Διαχειριστής Συστημάτων και Δικτύου	Β
Προγραμματιστής	Α, Η
Διευθυντής Ασφάλειας Πληροφοριών	Β, Γ
Διευθυντής Ανθρώπινου Δυναμικού	Α
Νομικός Σύμβουλος	Α
Διευθυντής Διαχείρισης Εγκαταστάσεων	Γ
Υπεύθυνος Φυσικής Ασφάλειας	Γ
Συνεργείο Καθαρισμού	Ε
Εσωτερικός Ελεγκτής	Δ
Επισκέπτης	Ζ

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 009: Σύστημα διαχείρισης κωδικών πρόσβασης

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θα καθιερωθούν κανόνες διαχείρισης των κωδικών πρόσβασης στα συστήματα και τις εφαρμογές.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι ο καθορισμός κανόνων διαχείρισης των κωδικών πρόσβασης στα συστήματα και τις εφαρμογές, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.9.3.1, Α.9.4.3

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από όλο το προσωπικό.

4. Πολιτική

Όλοι οι κωδικοί πρόσβασης πρέπει να έχουν τα παρακάτω χαρακτηριστικά:

- Να είναι μοναδικοί
- Να αποτελείται από τουλάχιστον 14 αλφαριθμητικούς χαρακτήρες
- Να περιλαμβάνει πεζούς και κεφαλαίους χαρακτήρες
- Να περιλαμβάνει τουλάχιστον δύο αριθμούς
- Να περιλαμβάνει τουλάχιστον δύο σύμβολα

Η αλλαγή των κωδικών πρόσβασης πρέπει να γίνεται κάθε 3 μήνες. Αν υπάρχει υπόνοια ότι ο κωδικός διέρρευσε σε μη εξουσιοδοτημένα άτομα τότε πρέπει να γίνει η αλλαγή του άμεσα και να αναφερθεί το περιστατικό στον διευθυντή ασφάλειας πληροφοριών.

Όπου υπάρχει η δυνατότητα πρέπει να χρησιμοποιείται η υπηρεσία αυθεντικοποίηση δυο παραγόντων (Two Factor Authentication)

Πρέπει να γίνεται χρήση ασφαλούς εφαρμογής διαχειριστή κωδικών για την διαχείριση των στοιχείων πρόσβασης των χρηστών.

Οι κωδικοί πρόσβασης δεν θα πρέπει:

- Να καταγράφονται σε χαρτί
- Να λέγονται φωναχτά
- Να αποστέλλονται μέσω email, SMS, messenger, κτλ.
- Να αναγράφονται σαν απλό κείμενο σε αρχεία πηγαίου κώδικα, scripts ή αρχεία ρυθμίσεων.
- Να αποκαλύπτονται σε άλλα άτομα (ακόμα και σε προϊστάμενους)
- Να επαναχρησιμοποιούνται
- Να είναι τα ίδιοι σε όλα τα συστήματα
- Να αποθηκεύονται μέσω της λειτουργίας ορισμένων εφαρμογών «Remember Password»
- Να ελέγχονται σε online υπηρεσίες ελέγχου κωδικών.
- Να είναι οι εξορισμού από τον κατασκευαστή.

Δεν επιτρέπετε η αυτόματη εισαγωγή (Automatic Log-in) σε υπηρεσίες και συστήματα.

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης, μέσω εργαλείων διαχείρισης συστημάτων, μέσω περιοδικών Penetration testing ή με τυχαίους δειγματοληπτικούς ελέγχους που θα διενεργεί ο οργανισμός.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 010: Χρήση κρυπτογράφησης

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θα καθιερωθούν κανόνες για την χρήση ελέγχων κρυπτογράφησης στα συστήματα και τις εφαρμογές του οργανισμού.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι ο καθορισμός κανόνων για την χρήση ελέγχων κρυπτογράφησης στα συστήματα και τις εφαρμογές του οργανισμού ούτος ώστε ευαίσθητα δεδομένα που διακινούνται, να μην μπορούν να διαβαστούν από μη εξουσιοδοτημένα άτομα, διασφαλίζοντας με αυτό τον τρόπο την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς επίσης τη συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.10.1.1, Α.10.1.2

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από όλο το προσωπικό και συνεργάτες (εσωτερικούς ή εξωτερικούς).

4. Πολιτική

Όταν πρόκειται να μεταδοθούν ή αποθηκευτούν εμπιστευτικά προσωπικά/ευαίσθητα δεδομένα, τότε πρέπει να γίνεται χρήση των παρακάτω αλγορίθμων κρυπτογράφησης:

Αλγόριθμοι τμήματος (συμμετρική κρυπτογράφηση):

Χρήση του αλγορίθμου AES (Advanced Encryption Standard) ή άλλου αλγόριθμου συμβατού με AES (π.χ. Twofish) σύμφωνα με το κείμενο «IETF/IRTF Ciphers in Use in the Internet» (Παράγραφοι 3.1 και 4.7) [18].

Προτεινόμενες Εφαρμογές/APIs/Libraries:

- BitLocker (Windows OS)
- LUKS (Linux OS)
- KeePass (Password Manager)
- VeraCrypt (Virtual Encrypted Disks)
- GPG
- JCA/JCE (Java Cryptography Architecture/Java Cryptography Extension)

Αλγόριθμοι δημοσίου κλειδιού (ασύμμετρη κρυπτογράφηση):

Πρέπει να πληρούν τις απαιτήσεις της τελευταίας έκδοσης του προτύπου του NIST «FIPS 140-2». Προτείνεται η χρήση του αλγορίθμου RSA (Rivest–Shamir–Adleman), αλγορίθμων ελλειπτικών καμπυλών (Elliptic Curve Cryptography) ή συνδυασμός αυτών με τον αλγόριθμο AES [18]. Επιπλέον, η εγκυρότητα των δημοσίων κλειδιών πρέπει να γίνετε από ανεξάρτητη, έγκυρη υποδομή δημοσίου κλειδιού (PKI).

Προτεινόμενες Εφαρμογές/APIs/Libraries:

- GPG

- JCA/JCE (Java Cryptography Architecture/Java Cryptography Extension)
- SSL/TLS (με Diffie–Hellman ή Elliptic-curve Diffie–Hellman key exchange)

Αλγόριθμοι ψηφιακών υπογραφών:

Χρήση του αλγορίθμου RSA ή αλγορίθμων ελλειπτικών καμπυλών (Elliptic Curve Cryptography). Όλα τα δεδομένα που μεταδίδονται κρυπτογραφημένα προς τον οργανισμό, πρέπει να είναι ψηφιακά υπογεγραμμένα και να γίνεται η πιστοποίηση της ταυτότητας του αποστολέα [18].

Αλγόριθμοι κατακερματισμού:

Χρήση του αλγόριθμου SHA-256 ή SHA-512.

Αποθήκευση κλειδιών:

Η αποθήκευση των κλειδιών κρυπτογράφησης (συμπεριλαμβανομένου και των αντίγραφων ασφαλείας), πρέπει να γίνεται σε κρυπτογραφημένο μέσο αποθήκευσης (HDD, SSD, USB disk, Virtual Encrypted Disk, κτλ.).

Προτεινόμενες Εφαρμογές/APIs/Libraries:

- KeyTool (Java key and certificate management utility). Δημιουργία KeyStores τύπου JCEKS. Τα κλειδιά αποθηκεύονται κρυπτογραφημένα με την χρήση του αλγόριθμου 3DES.

Διάρκεια ζωής μυστικών κλειδιών:

Η διάρκεια ζωής των μυστικών κλειδιών πρέπει να είναι: 1 χρόνος.

Αν υπάρχει υπόνοια ότι το μυστικό κλειδί διέρρευσε σε μη εξουσιοδοτημένα άτομα τότε πρέπει να γίνει η αλλαγή του άμεσα και να αναφερθεί το περιστατικό στον διευθυντή ασφάλειας πληροφοριών.

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 011: Καθαρό γραφείο/καθαρή οθόνη

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι το προσωπικό του οργανισμού δεν θα αφήνει ευαίσθητες πληροφορίες εκτεθειμένες στον χώρο εργασίας τους.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η διασφάλιση ότι το προσωπικό του οργανισμού δεν θα αφήνει ευαίσθητες πληροφορίες εκτεθειμένες στον χώρο εργασίας τους, καθώς επίσης τη συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.11.2.8, Α.11.2.9

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από όλο το προσωπικό.

4. Πολιτική

1. Οι κωδικοί πρόσβασης δεν πρέπει να είναι εκτεθειμένοι πάνω στο γραφείο γραμμένοι σε χαρτί.
2. Όλες οι ευαίσθητες/εμπιστευτικές πληροφορίες (ηλεκτρονικές ή έντυπες), πρέπει να βρίσκονται σε ασφαλές μέρος μετά το πέρας της εργασίας του προσωπικού (Διαδικασία 003).
3. Όλες οι έντυπες ευαίσθητες/εμπιστευτικές πληροφορίες, πρέπει να αφαιρούνται άμεσα από τον εκτυπωτή μετά την εκτύπωση τους [18].
4. Κλειδιά και Smartcards για πρόσβαση σε εγκαταστάσεις του οργανισμού, δεν πρέπει να βρίσκονται χωρίς επιτήρηση. Πρέπει να βρίσκονται σε ασφαλές μέρος μετά το πέρας της εργασίας του προσωπικού [18].
5. Πρέπει να τερματίζεται η λειτουργία όλων των σταθμών εργασίας (Workstations/Laptops) μετά το πέρας της εργασίας του προσωπικού.
6. Οι σταθμοί εργασίας πρέπει να μπαίνουν σε λειτουργία κλειδώματος με προστασία οθόνης σε περίπτωση ολιγόωρης απουσίας ή διαλλείματος. Αυτό πρέπει να γίνεται και αυτόματα σε περίπτωση που ο σταθμός εργασίας μείνει σε αδράνεια μετά από τον χρόνο που ορίζεται στην πολιτική 013 [18].
7. Εξοπλισμός που είναι χωρίς συνεχή επιτήρηση (π.χ. Servers) πρέπει να βρίσκεται συνεχώς σε λειτουργία κλειδώματος με προστασία οθόνης.
8. Οι φορητοί υπολογιστές πρέπει να είναι κλειδωμένοι πάνω στο γραφείο με το κατάλληλο καλώδιο [18].
9. Ευαίσθητες/εμπιστευτικές πληροφορίες που βρίσκονται γραμμένες πάνω σε πίνακες κατά την διάρκεια εκπαίδευσης ή άλλης δραστηριότητας (π.χ. καταγραφή ιδεών) πρέπει να σβήνονται στο τέλος της εργάσιμης ημέρας.

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 012: Τήρηση αρχείων καταγραφής συμβάντων

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θα τηρούνται αρχεία καταγραφής συμβάντων (event logging) από συστήματα, υπηρεσίες, εφαρμογές και mobile agents.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η διασφάλιση ότι θα τηρούνται αρχεία καταγραφής συμβάντων από συστήματα, υπηρεσίες, εφαρμογές και mobile agents, καθώς επίσης τη συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.12.4.1, Α.12.4.2, Α.12.4.3, Α.12.4.4

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από τους:

- Διαχειριστή Συστημάτων και Δικτύων
- Προγραμματιστές

4. Πολιτική

Όλες οι λειτουργίες καταγραφής συμβάντων πρέπει να είναι ενεργοποιημένες και η παρακολούθηση τους πρέπει να γίνεται κεντρικά από τον διαχειριστή συστημάτων και δικτύων για τυχόν περιστατικά που αφορούν την ασφάλεια.

Όσο αφορά την ανάπτυξη mobile agents, πρέπει να υλοποιείται η καταγραφή συμβάντων από τους προγραμματιστές (και ανεξάρτητα από το αρχείο καταγραφής συμβάντων της πλατφόρμας). Στα αρχεία πρέπει να καταγράφεται:

- Αναγνωριστικό (ID) του mobile agent
- Ημερομηνία/ώρα δημιουργία του mobile agent
- Ημερομηνία/ώρα αποστολής του mobile agent
- Ημερομηνία/ώρα συμβάντων που αφορούν την εκτέλεση του mobile agent στον απομακρυσμένο host (π.χ. κρυπτογράφηση δεδομένων, η λήψη των δεδομένων, κ.α.)
- Χρόνος εκτέλεσης και επιστροφής του mobile agent
- Αποκρυπτογράφηση / Έλεγχος ακεραιότητας των δεδομένων.

Τα αρχεία καταγραφής συμβάντων θα προστατεύονται μέσω:

- Των κρυπτογραφημένων μέσων αποθήκευσης των συστημάτων (Πολιτική 013)
- Της πολιτικής καθαρού γραφείου/καθαρής οθόνης (Πολιτική 011)
- Του ελέγχου πρόσβασης χρηστών στα συστήματα (Πολιτική 013)

Πρέπει να γίνεται αυτόματος συγχρονισμός των ρολογιών όλων των hosts μέσω του time server (NTP) της Microsoft time.windows.com

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 013: Προφίλ ασφάλειας υπολογιστικών συστημάτων

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι σε όλα τα υπολογιστικά συστήματα του οργανισμού θα εφαρμόζονται προφίλ ασφάλειας για διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι ο καθορισμός των προφίλ ασφάλειας των υπολογιστικών συστημάτων του οργανισμού, καθώς επίσης τη συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: A.11.2.6, A.12.1.3, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από τους:

- Διαχειριστή Συστημάτων και Δικτύων

4. Πολιτική

Κατά την ρύθμιση/εγκατάσταση υπολογιστικών συστημάτων πρέπει να εφαρμόζονται τα παρακάτω προφίλ:

Controls	Work Stations	Laptops	Production Hosts	Test Hosts	Backup NAS	SVN Server
Κρυπτογράφηση Δίσκου	✓	✓	✓	✓	✓	✓
Απενεργοποίηση USB Ports	✗	✗	✓	✗	✓	✓
Εγκατάσταση Anti-virus/Anti-ransomware με ενεργοποιημένες τις αυτόματες ενημερώσεις	✓	✓	✓	✓	✓	✓
Εγκατάσταση UPS	✓	✓	✓	✓	✓	✓
Screen Saver Timeout	3 min	2 min	1 min	1 min	1 min	1 min
Lock Screen Timeout	3 min	2 min	1 min	1 min	1 min	1 min
Εγκατάσταση Password Manager	✓	✓	✗	✗	✗	✗
Τήρηση αντιγράφων ασφαλείας στον Backup NAS	✓	✓	✓	✗	✗	✓
Παρακολούθηση Χωρητικοτήτων και λήψη διορθωτικών μέτρων έγκαιρα.	✓	✓	✓	✓	✓	✓
Παρακολούθηση αρχείων καταγραφής συμβάντων	✓	✓	✓	✓	✓	✓
Ενημερώσεις Ασφαλείας Λογισμικού (OS, Software)	✓	✓	✓	✓	✓	✓
Αναβαθμίσεις Hardware (όποτε θεωρηθεί αναγκαίο)	✓	✓	✓	✓	✓	✓

Επιπλέον:

- Δεν πρέπει να γίνεται εγκατάσταση λογισμικού που δεν έχει εγκριθεί από τον διευθυντή ασφάλειας πληροφοριών (Αρχείο καταγραφής 004) και δεν έχει σχέση με την λειτουργία του οργανισμού.
- Δεν πρέπει να γίνεται εγκατάσταση λογισμικού με κακή φήμη.
- Δεν πρέπει να γίνεται εγκατάσταση λογισμικού χωρίς έγκυρη και νόμιμη άδεια χρήσης.
- Πριν τις αναβαθμίσεις λογισμικού/hardware πρέπει να διασφαλίζεται και να λαμβάνεται υπόψιν η συμβατότητα της ενημέρωσης με το υπόλοιπο εγκατεστημένο λογισμικό αλλά και με τα υπόλοιπα συστήματα του οργανισμού.

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 014: Απαιτήσεις ελέγχων επιθεώρησης υπολογιστικών συστημάτων

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θα γίνονται τακτικές επιθεωρήσεις της σωστής λειτουργίας των υπολογιστικών συστημάτων βάση ορισμένων απαιτήσεων.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι ο καθορισμός των απαιτήσεων για τακτικές επιθεωρήσεις της λειτουργίας των υπολογιστικών συστημάτων, καθώς επίσης τη συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.12.7.1

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από τους:

- Διαχειριστή Συστημάτων και Δικτύων
- Διευθυντή Ασφάλειας Πληροφοριών
- Υπεύθυνο Φυσικής Ασφάλειας

4. Πολιτική

Ο οργανισμός πρέπει να διενεργεί τις παρακάτω επιθεωρήσεις συστημάτων:

Επιθεώρηση	Συχνότητα	Υπεύθυνος
Penetration Testing (Συστήματα)	Κάθε 6 μήνες	Διευθυντής Ασφάλειας Πληροφοριών
Penetration Testing (Εγκαταστάσεις)	Κάθε 6 μήνες	Υπεύθυνος Φυσικής Ασφάλειας
Έλεγχος σωστής λειτουργίας CCTV, πυρασφάλειας, αντιπλημμυρικού συστήματος	Κάθε 3 μήνες	Υπεύθυνος Φυσικής Ασφάλειας
Διαχείριση Συστημάτων και Δικτύων • Παρακολούθηση και ανάλυση κίνησης δικτύου • Παρακολούθηση επισκεψιμότητας ύποπτων σελίδων (π.χ. file sharing) από το προσωπικό • Παρακολούθηση και ανάλυση Antivirus • Παρακολούθηση Χωρητικοτήτων • Εγκατάσταση/Αναβάθμιση εφαρμογών. • Έλεγχος πρόσβασης στα συστήματα. • Ανάλυση αρχείων καταγραφής (log files).	Κάθε μέρα	Διαχειριστής Συστημάτων και Δικτύων

• Καταγραφή , αναφορά και αντιμετώπιση περιστατικών ασφαλείας. • Διασφάλιση απρόσκοπτης παροχής ηλεκτρικού ρεύματος στα συστήματα • Συντήρηση εξοπλισμού.		
Έλεγχος δικαιωμάτων πρόσβασης mobile agents άλλων πρακτορείων.	Κάθε 3 μήνες	Διαχειριστής Συστημάτων και Δικτύων

Σε περίπτωση που βρεθούν κενά ασφάλειας πρέπει το υπεύθυνο προσωπικό να προβαίνει σε διορθωτικές ενέργειες άμεσα. Για την κάθε επιθεώρηση πρέπει να συντάσσετε αναλυτική αναφορά με τα ευρήματα και να αποστέλνεται στην διοίκηση.

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 015: Ασφάλεια δικτύου

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θα εφαρμόζονται οι κατάλληλοι έλεγχοι για την ασφάλεια του δικτύου του οργανισμού.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η εφαρμογή των κατάλληλων ελέγχων για την ασφάλεια του δικτύου του οργανισμού, καθώς επίσης τη συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.11.2.3, Α.13.1.1, Α.13.1.2

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από τους:

- Διοίκηση
- Διαχειριστή Συστημάτων και Δικτύων

4. Πολιτική

Ο οργανισμός πρέπει να εφαρμόζει τα παρακάτω για την ασφάλεια του τοπικού δικτύου:

- Απενεργοποίηση της λειτουργιών ασύρματου δικτύου (Wi-Fi & bluetooth).
- Απαγορεύεται η πρόσβαση στο δίκτυο του οργανισμού ως επισκέπτης (Guest)
- Εγκατάσταση Anti-virus/Anti-ransomware σε όλα τα υπολογιστικά συστήματα.
- Εκπαίδευση του προσωπικού σε θέματα ασφάλειας (π.χ. αναγνώριση phishing email, social engineering, κ.α.).
- Διαχωρισμός των δικτύων του κάθε τμήματος με χρήση VLANs ώστε κάθε τμήμα να μην έχει πρόσβαση στο δίκτυο κάποιου άλλου.
- Εγκατάσταση και ρύθμιση του firewall με τέτοιο τρόπο ώστε να υπάρχει επικοινωνία μόνο με εφαρμογές και υπηρεσίες που χρησιμοποιεί ο οργανισμός. Οποιαδήποτε άλλη επικοινωνία πρέπει να μπλοκάρεται αυτόματα.
- Εγκατάσταση και ρύθμιση φίλτρου περιεχομένου διαδικτύου (Web Content Filter) που θα επιτρέπει πρόσβασή μόνο σε ιστοσελίδες που έχουν να κάνουν με την δραστηριότητα του οργανισμού.
- Εγκατάσταση και ρύθμιση συστημάτων εντοπισμού και έγκαιρης αποτροπής εισβολέων (IDS/IPS).
- Αναβαθμίσεις ασφαλείας για όλα τα συστήματα του δικτύου (π.χ. routers)
- Όλες οι καλωδιώσεις του δικτύου πρέπει να είναι εντοιχισμένες. Πρέπει να χρησιμοποιούν ξεχωριστές σωληνώσεις παράλληλα με τις καλωδιώσεις της ηλεκτρολογικής εγκατάστασης.
- Όλοι οι Servers πρέπει να είναι ασφαλισμένοι μέσα σε ιδικά δωμάτια και Racks και με τον κατάλληλο κλιματισμό.

Για κάθε μία από τις υπηρεσίες του δικτύου (Mobile Agent Platform, VPN, VLANs, Router/Switches, Firewall, IPS/IDS, κτλ.) πρέπει να υπάρχει συμφωνία επιπέδου υπηρεσίας (Service Level Agreement ή SLA) από τον πάροχο της. Ορισμένα στοιχεία που πρέπει να περιλαμβάνει ένα SLA είναι:

- Να παρέχονται ασφαλείς μηχανισμοί ασφαλείας της υπηρεσίας (π.χ. κρυπτογράφηση, two step authentication, κτλ.) που να είναι συμβατοί με τις πολιτικές του οργανισμού.
- Να παρέχονται ενημερώσεις ασφαλείας της υπηρεσίας.
- 24ωρη υποστήριξη.
- Επίλυση προβλημάτων εντός 48 ωρών

Η απόδοση των υπηρεσιών που παρέχονται από τρίτους, πρέπει να παρακολουθείται από τον οργανισμό.

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 016: Ασφάλεια στην ανάπτυξη λογισμικού

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θα εφαρμόζονται οι κατάλληλοι έλεγχοι για την ασφαλή ανάπτυξη λογισμικού στον οργανισμό.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η εφαρμογή των κατάλληλων ελέγχων για την ασφαλή ανάπτυξη λογισμικού στον οργανισμό, καθώς επίσης τη συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.14.2.1, Α.14.2.2, Α.14.2.3, Α.14.2.4, Α.14.2.5, Α.14.2.6, Α.14.2.8, Α.14.2.9, Α.14.3.1, Α.15.1.1

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από τους προγραμματιστές.

4. Πολιτική

Ο οργανισμός πρέπει να εφαρμόζει τα παρακάτω για την ασφαλή ανάπτυξη λογισμικού:

- Ανάλυση απαιτήσεων ασφαλείας δεδομένων κατά την διαδικασία του σχεδιασμού της εφαρμογής (Διαδικασία 008).
- Χρήση κρυπτογραφίας για την διασφάλιση της εμπιστευτικότητας και της ακεραιότητας κατά την μετάδοση ευαίσθητων δεδομένων από την εφαρμογή.
- Τήρηση εκδόσεων πηγαίου κώδικα μετά από την εφαρμογή αλλαγών (Version Control).
- Υλοποίηση συστήματος καταγραφής συμβάντων της εφαρμογής (πολιτική 012).
- Αναλυτικοί έλεγχοι λειτουργίας/ασφάλειας της εφαρμογής σε ειδικό περιβάλλον (Testing Hosts) πριν την διάθεσή της σε παραγωγικό σύστημα (Production Hosts). Οι έλεγχοι αυτοί πρέπει να γίνονται αρχικά με την δημιουργία της εφαρμογής αλλά και μετέπειτα μετά από αλλαγές ή/και αναβαθμίσεις.
- Μετά από κάθε έλεγχο εφαρμογής τόσο η εφαρμογή αλλά και τα παραγόμενα αποτελέσματα/δεδομένα πρέπει να διαγράφονται αυτόματα και με ασφαλή τρόπο από τα υπολογιστικά συστήματα δοκιμής (Testing Hosts), μετά το τέλος της ημέρας.
- Έγκαιρη αποσφαλμάτωση / κλείσιμο κενών ασφαλείας.
- Δεν πρέπει να γίνονται επεμβάσεις στις εφαρμογές/ πλατφόρμες/ βιβλιοθήκες/ περιβάλλοντα ανάπτυξης λογισμικού που παρέχονται από τρίτους (π.χ. στα IDEs).
- Πρέπει να υπάρχει διαδικασία που να εφαρμόζεται σε περίπτωση αλλαγής συστημάτων κατά την διάρκεια του κύκλου ζωής της εφαρμογής.
- Πριν γίνει οποιαδήποτε αλλαγή στα συστήματα του τμήματος ανάπτυξης λογισμικού, πρέπει να γίνονται τεχνικοί έλεγχοι, να λαμβάνεται υπόψιν η ασφάλεια και να γίνεται με τέτοιο τρόπο, ώστε να μην υπάρχει επίπτωση στην ομαλή λειτουργία του οργανισμού.

Επιπλέον οι προγραμματιστές πρέπει να ακολουθούν τις παρακάτω αρχές:

- Απαγορεύεται να εφαρμόζουν κακόβουλο κώδικα στις εφαρμογές.
- Απαγορεύεται να διαρρέουν σε τρίτους και με οποιοδήποτε τρόπο πηγαίο κώδικα της εφαρμογής ή παραγόμενα δεδομένα.

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 017: Οι Σχέσεις με τους προμηθευτές

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θα εφαρμόζονται οι κατάλληλοι έλεγχοι ασφαλείας κατά την συνεργασία του οργανισμού με τους προμηθευτές.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η εφαρμογή των κατάλληλων ελέγχων ασφαλείας κατά την συνεργασία του οργανισμού με τους προμηθευτές, καθώς επίσης τη συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από την διοίκηση.

4. Πολιτική

Ο οργανισμός πρέπει να εφαρμόζει τα παρακάτω για την ασφαλή συνεργασία με τους προμηθευτές:

- Υπογραφή συμφώνου εμπιστευτικότητας (NDA 001) σε περίπτωση που ο προμηθευτής θα χρειαστεί να έχει πρόσβαση στα περιουσιακά στοιχεία του οργανισμού.
- Υπογραφή συμφωνίας με κάθε προμηθευτή όπου θα καθορίζονται οι σχετικές απαιτήσεις ασφαλείας πρόσβασης, επεξεργασίας, αποθήκευσης και επικοινωνίας περιουσιακών στοιχείων του οργανισμού. Η συμφωνία πρέπει να περιλαμβάνει και τις απαιτούμενες γνώσεις/εκπαίδευσης που πρέπει να έχει ο προμηθευτής.
- Τακτική παρακολούθηση των προσφερόμενων υπηρεσιών από τους προμηθευτές.
- Με κάθε αλλαγή που γίνεται στις υπηρεσίες των προμηθευτών πρέπει να λαμβάνεται υπόψιν και να επανεκτιμάται ο κίνδυνος (Διαδικασία 006).

5. Συμμόρφωση με την Πολιτική

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Πολιτική 018: Τυχαίοι δειγματοληπτικοί έλεγχοι

1. Επισκόπηση

Με την πολιτική αυτή διασφαλίζεται ότι θα γίνονται τυχαίοι δειγματοληπτικοί έλεγχοι συμμόρφωσης με το ΣΔΑΠ.

2. Σκοπός

Ο σκοπός αυτής της πολιτικής είναι η πραγματοποίηση τυχαίων δειγματοληπτικών ελέγχων συμμόρφωσης με το ΣΔΑΠ.

Έλεγχοι από το Παράρτημα Α:

3. Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται από τον διευθυντή ασφάλειας πληροφοριών.

4. Πολιτική

Πρέπει να γίνονται τυχαίοι δειγματοληπτικοί έλεγχοι συμμόρφωσης με το ΣΔΑΠ. Όλες οι μη συμμορφώσεις πρέπει να καταγράφονται στο αρχείο καταγραφής 009.

Οι έλεγχοι μπορεί να γίνουν:

- Μετά από την ανακοίνωση νέων ευπαθειών, από έγκυρες πηγές.
- Κατά την διάρκεια μιας 'βόλτας' εντός του οργανισμού (site walk).

Πρέπει να γίνει παρακολούθηση της υλοποίησης των διορθωτικών ενεργειών (βάση του πλάνου).

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την πολιτική θα ελέγχεται μέσω της εσωτερικής επιθεώρησης.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την πολιτική θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Β.2 Διαδικασίες

Διαδικασία 001: Καθορισμός πολιτικών και διαδικασιών ασφάλειας πληροφοριών

1. **Επισκόπηση**

   Η διαδικασία του καθορισμού και ανασκόπησης των πολιτικών και διαδικασιών ασφάλειας πληροφοριών διασφαλίζει ότι όλοι οι εργαζόμενοι στον Οργανισμό ΧΥΖ θα ακολουθούν ορισμένους κανόνες που ως στόχο έχουν την ασφάλεια των πληροφοριών που επεξεργάζονται.

2. **Σκοπός**

   Ο σκοπός αυτής της διαδικασίας είναι η υλοποίηση των πολιτικών και διαδικασιών ασφαλείας καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

   Έλεγχοι από το Παράρτημα Α: Α.5.1.1, Α.5.1.2

3. **Πεδίο Εφαρμογής**

   Αυτή την διαδικασία εφαρμόζεται από τον Διευθυντή Ασφάλειας Πληροφοριών.

4. **Διαδικασία**

   - Καθορισμός Πολιτικών Ασφάλειας

     4.1. Μελέτη απαιτήσεων ασφαλείας όπως αυτές καθορίστηκαν στην παράγραφο 4.2 του ISO 27001.
     4.2. Μελέτη των αποτελεσμάτων της Αξιολόγησης Κινδύνων (Παράγραφος 6.1.2 του ISO 27001)
     4.3. Συγγραφή της πολιτικής ασφαλείας ή της διαδικασίας.
     4.4. Έγκριση της πολιτικής ή διαδικασίας ασφαλείας από την διοίκηση.
     4.5. Εκπαίδευση του προσωπικού που αφορά η εκάστοτε πολιτική ή διαδικασία. Συμπλήρωση του αρχείο καταγραφής 007.

   - Ανασκόπηση Πολιτικών και Διαδικασιών Ασφάλειας

     Η ανασκόπηση των πολιτικών ασφαλείας πρέπει να γίνεται κάθε 6 μήνες ή όποτε προκύψει ανάγκη για άμεση λήψη διορθωτικών ενεργειών.

     Η ανασκόπηση των διαδικασιών ασφαλείας πρέπει να γίνεται κάθε 3 μήνες ή όποτε προκύψει ανάγκη για άμεση λήψη διορθωτικών ενεργειών.

   - Επικοινωνία Πολιτικών και Διαδικασιών Ασφάλειας

     Η επικοινωνία για την αποστολή των πολιτικών και διαδικασιών ασφαλείας (η των ενημερωμένων εκδόσεων) πρέπει να γίνεται μέσω ηλεκτρονικού ταχυδρομείου με χρήση κρυπτογράφησης (SSL/TLS). Στην συνέχεια πρέπει να ενημερώνεται το σχετικό αρχείο (Αρχείο Καταγραφής 008).

5. **Συμμόρφωση με την Διαδικασία**

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Διαδικασία 002: Πειθαρχική διαδικασία

1. Επισκόπηση

Η πειθαρχική διαδικασία διασφαλίζει ότι όλοι οι εργαζόμενοι στον Οργανισμό XYZ θα έχουν πειθαρχικές επιπτώσεις σε περίπτωση πρόκλησης περιστατικού ασφάλειας κατά την άσκηση των καθηκόντων τους.

2. Σκοπός

Ο σκοπός αυτής της διαδικασίας είναι η υλοποίηση μιας πειθαρχικής διαδικασίας που να αποτρέπει τους εργαζόμενους από το να προκαλέσουν περιστατικό ασφάλειας λόγο μη εφαρμογής των πολιτικών ασφάλειας ή παραβίασης του συμβολαίου ή NDA, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.7.2.3

3. Πεδίο Εφαρμογής

Αυτή την διαδικασία εφαρμόζεται από την διοίκηση και όλους τους διευθυντές τμημάτων.

4. Διαδικασία

- Μικρά παραπτώματα:

    1. Στάδιο 1: Προφορική προειδοποίηση
    2. Στάδιο 2: 1η γραπτή προειδοποίηση
    3. Στάδιο 3: 2η γραπτή προειδοποίηση
    4. Στάδιο 4: 3η γραπτή προειδοποίηση
    5. Στάδιο 5: Τερματισμός Απασχόλησης ή λήψη άλλων μέτρων

- Μεγάλα παραπτώματα:

    1. Στάδιο 1: γραπτή προειδοποίηση
    2. Στάδιο 2: Τερματισμός Απασχόλησης ή λήψη άλλων μέτρων

- Πολύ σοβαρά παραπτώματα:

    1. Βήμα 1: Ενημέρωση του εργαζόμενου σχετικά με τους ισχυρισμούς
    2. Βήμα 2: Έρευνα σχετικά με το περιστατικό και συλλογή αποδεικτικών στοιχείων.
    3. Βήμα 3: Πειθαρχική ακρόαση
    4. Βήμα 4: Τερματισμός Απασχόλησης ή/και λήψη άλλων μέτρων (π.χ. νομικών)

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Διαδικασία 003: Χειρισμός περιουσιακών στοιχείων

1. Επισκόπηση

Η διαδικασία καθορίζει τον χειρισμό (επεξεργασία, αποθήκευση και μετάδοση) των περιουσιακών στοιχείων του οργανισμού βάση της διαβάθμισης τους.

2. Σκοπός

Η διαδικασία αυτή έχει ως σκοπό να καθορίσει τον χειρισμό των περιουσιακών στοιχείων του οργανισμού, ώστε να διασφαλίζεται η εμπιστευτικότητα, ακεραιότητα και η διαθεσιμότητα τους, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: A.8.2.3, A.8.3.1 , A.8.3.2, A.8.3.3, 11.2.7

3. Πεδίο Εφαρμογής

Αυτή την διαδικασία εφαρμόζεται από όλο το προσωπικό που χειρίζεται περιουσιακά στοιχεία του οργανισμού.

4. Διαδικασία

Επεξεργασία:

Η επεξεργασία των διαβαθμισμένων περιουσιακών στοιχείων μπορεί να γίνει μόνο από άτομα που καθορίζονται στο επίσημο «μητρώο εξουσιοδοτημένων αποδεκτών περιουσιακών στοιχείων» (Αρχείο Καταγραφής 003).

Αποθήκευση:

Η αποθήκευση των περιουσιακών στοιχείων γίνεται σε ειδικό διαμορφωμένο μέρος και από εξουσιοδοτημένα άτομα που έχουν πρόσβαση σε αυτό.

Περιουσιακό Στοιχείο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης	Εσωτερικής Χρήσης
Έγγραφο	Αποθηκευτικός Χώρος Εγγράφων & Μέσων Αποθήκευσης	Αποθηκευτικός Χώρος Εγγράφων & Μέσων Αποθήκευσης	Αποθηκευτικός Χώρος Εγγράφων & Μέσων Αποθήκευσης / σιτάρι γραφείου (που κλειδώνει)	Αποθηκευτικός Χώρος Εγγράφων & Μέσων Αποθήκευσης/ σιτάρι γραφείου (που κλειδώνει)
Ηλεκτρονικό έγγραφο	Κρυπτογραφημένο μέσο αποθήκευσης	Κρυπτογραφημένο μέσο αποθήκευσης	Κρυπτογραφημένο μέσο αποθήκευσης	Κρυπτογραφημένο μέσο αποθήκευσης
E-Mail	Κρυπτογραφημένο μέσο αποθήκευσης	Κρυπτογραφημένο μέσο αποθήκευσης	Κρυπτογραφημένο μέσο αποθήκευσης	Κρυπτογραφημένο μέσο αποθήκευσης
Μέσο αποθήκευσης	Αποθηκευτικός Χώρος Εγγράφων & Μέσων Αποθήκευσης	Αποθηκευτικός Χώρος Εγγράφων & Μέσων Αποθήκευσης	Αποθηκευτικός Χώρος Εγγράφων & Μέσων Αποθήκευσης	Αποθηκευτικός Χώρος Εγγράφων & Μέσων Αποθήκευσης
Κώδικας	Κρυπτογραφημένο μέσο αποθήκευσης	Κρυπτογραφημένο μέσο αποθήκευσης	Κρυπτογραφημένο μέσο αποθήκευσης	Κρυπτογραφημένο μέσο αποθήκευσης

Προφορική πληροφορία	N/A	N/A	N/A	N/A

Μετάδοση:

Η κοινοποίηση των περιουσιακών στοιχείων του οργανισμού, μπορεί να γίνει μόνο από άτομα που καθορίζονται στο επίσημο «μητρώο εξουσιοδοτημένων αποδεκτών περιουσιακών στοιχείων» και αφού ληφθεί σχετική άδεια από τον διευθυντή του τμήματος.

Καταστροφή / επαναχρησιμοποίηση μέσου αποθήκευσης:

Όλα τα μέσα αποθήκευσης πρέπει να καταστρέφονται όταν πια δεν χρησιμοποιούνται και πρέπει να γίνεται με τον εξής τρόπο:

1. Αποστολή σχετικής αίτησης στον Διευθυντή Ασφάλειας Πληροφοριών. Η αίτηση πρέπει να αναφέρει τους λόγους καταστροφής.
2. Λήψη εξουσιοδότησης από τον Διευθυντή Ασφάλειας Πληροφοριών
3. Διαγραφή δεδομένων κάνοντας χρήση ιδικού λογισμικού. Αν το μέσο αποθήκευσης είναι σε κατάσταση που μπορεί να επαναχρησιμοποιηθεί τότε δεν προχωράμε στο επόμενο βήμα.
4. Παραλαβή και καταστροφή μέσου από τον Υπεύθυνο Φυσικής Ασφάλειας χρησιμοποιώντας τον κατάλληλο εξοπλισμό (Καταστροφέας Εγγράφων & Καταστροφέας Μέσων Αποθήκευσης). Στην συνέχεια τα κατεστραμμένα μέσα αποθήκευσης, στέλνονται για ανακύκλωση. Αν δεν εγκριθεί η καταστροφή του τότε το μέσο αποθηκεύεται στον Αποθηκευτικό Χώρο Εγγράφων & Μέσων Αποθήκευσης.

Φυσική μεταφορά μέσου αποθήκευσης:

Η φυσική μεταφορά του μέσου αποθήκευσης μπορεί να γίνει με δύο τρόπους:

- Με την Βαλίτσα Ασφαλείας Μεταφοράς Εγγράφων.
- Με την χρήση εταιριών courier που παρέχουν ασφαλή μεταφορά αντικειμένων και εγγράφων.

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Διαδικασίες 004: Διαχείριση πρόσβασης χρηστών

1. Επισκόπηση

Η διαδικασία καθορίζει τον τρόπο με τον οποίο θα γίνεται η διαχείριση της πρόσβασης των χριστών στα διάφορα συστήματα, δίκτυα και εγκαταστάσεις.

2. Σκοπός

Η διαδικασία αυτή έχει ως σκοπό να καθορίσει τον τρόπο με τον οποίο θα γίνεται η διαχείριση της πρόσβασης των χριστών στα διάφορα συστήματα, δίκτυα και εγκαταστάσεις, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.9.2.1, Α.9.2.2, Α.9.2.6, , Α.9.4.4

3. Πεδίο Εφαρμογής

Αυτή την διαδικασία εφαρμόζεται από τους:

- Διαχειριστή Συστημάτων και Δικτύου
- Υπεύθυνο Φυσικής Ασφάλειας
- Διευθυντή Ασφάλειας Πληροφοριών

4. Διαδικασίες

4.1 Εγγραφή σε ηλεκτρονικές υπηρεσίες

Η εγγραφή στις υπηρεσίες γίνεται από τον Διαχειριστή Συστημάτων και Δικτύου μετά από σχετική γραπτή έγκριση του Διευθυντή Ασφάλειας Πληροφοριών.

4.1.1 Δημιουργία username ακολουθώντας τον κανόνα ονομα.επίθετο
4.2.2 Δημιουργία προσωρινού κωδικού πρόσβασης σύμφωνα με την πολιτική δημιουργίας δυνατών κωδικών.
4.2.3 Απονομή δικαιωμάτων πρόσβασης στο σύστημα σύμφωνα με το προφίλ του χρήστη στην πολιτική 008
4.2.4 Ενημέρωση του χρήστη με τα στοιχεία πρόσβασης.
4.2.5 Αλλαγή του προσωρινού κωδικού πρόσβασης από τον χρήστη άμεσα, σύμφωνα με την πολιτική δημιουργίας δυνατών κωδικών και ενημέρωση της εφαρμογής διαχείρισης κωδικών στον υπολογιστή του (workstation).

4.2 Διαγραφή/Προσαρμογή δικαιωμάτων από ηλεκτρονικές υπηρεσίες

Η διαγραφή/προσαρμογή δικαιωμάτων από τις υπηρεσίες γίνεται από τον Διαχειριστή Συστημάτων και Δικτύου μετά από σχετική γραπτή έγκριση του Διευθυντή Ασφάλειας Πληροφοριών. Σε περίπτωση τερματισμού της εργοδότησης, χρειάζεται γραπτή έγκριση και από τον Διευθυντή Ανθρώπινου Δυναμικού.

4.3 Πρόσβαση στις εγκαταστάσεις

Το δικαίωμα πρόσβασης στις εγκαταστάσεις του οργανισμού γίνεται από τον Υπεύθυνο Φυσικής Ασφάλειας μετά από σχετική γραπτή έγκριση του Διευθυντή Ασφάλειας Πληροφοριών. Ο Υπεύθυνος Φυσικής Ασφάλειας εκδίδει σχετική κάρτα πρόσβασης στις εγκαταστάσεις (γραφεία) του οργανισμού σύμφωνα με το προφίλ του χρήστη στην

πολιτική 008, ενώ εκτελούνται και οι διαδικασίες σάρωσης των δακτυλικών αποτυπωμάτων για την πρόσβαση στην είσοδο του οργανισμού.

4.4 Αφαίρεση δικαιωμάτων πρόσβασης στις εγκαταστάσεις

Η αφαίρεση δικαιωμάτων πρόσβασης στις εγκαταστάσεις (ακύρωση κάρτας) γίνεται από τον Υπεύθυνο Φυσικής Ασφάλειας μετά από σχετική γραπτή έγκριση του Διευθυντή Ασφάλειας Πληροφοριών. Σε περίπτωση τερματισμού της εργοδότησης χρειάζεται γραπτή έγκριση και από τον Διευθυντή Ανθρώπινου Δυναμικού.

4.5 Διαχείριση προνομιακών δικαιωμάτων πρόσβασης

Η διαχείριση των προνομιακών δικαιωμάτων πρόσβασης (Administrator Username/Password) στα συστήματα, πρέπει να γίνεται μέσω ασφαλούς εφαρμογής διαχείρισης κωδικών (π.χ. KeePass). Πρόσβαση στο Master Key της εφαρμογής Έχουν οι:

- Ο Διαχειριστής Συστημάτων και Δικτύου
- Ο Διευθυντής Ασφάλειας Πληροφοριών
- Η Διοίκηση

4.6 Διαχείριση στοιχείων πρόσβασης χρηστών

Η διαχείριση των στοιχείων πρόσβασης χρηστών στα συστήματα (username/password) πρέπει να γίνετε από τον διαχειριστή συστημάτων και δικτύου μέσω ενός κεντρικού συστήματος διαχείρισης (π.χ. Active Directory).

Η διαχείριση των στοιχείων πρόσβασης χρηστών (username/password) σε εφαρμογές (π.χ. Aglets) πρέπει να γίνεται χειροκίνητα, από τον διαχειριστή συστημάτων και δικτύου μέσω ασφαλούς εφαρμογής διαχείρισης κωδικών (π.Χ. KeePass).

Οι εφαρμογές ή τα συστήματα που προμηθεύονται με προ εγκατεστημένα στοιχεία πρόσβασης (default username/password), αυτά πρέπει να αλλάζουν άμεσα από τον διαχειριστή συστημάτων και δικτύου, πριν την εφαρμογή τους σε περιβάλλον παραγωγής.

4.7 Χρήση εφαρμογών με προνομιακά δικαιώματα πρόσβασης

Η χρήση εφαρμογών με προνομιακά δικαιώματα πρόσβασης πρέπει να γίνεται πάντα υπό την επίβλεψη του διαχειριστή συστημάτων και δικτύου.

4.8 Ανασκόπηση δικαιωμάτων πρόσβασης χρηστών

Η ανασκόπηση δικαιωμάτων πρόσβασης των χρηστών στα συστήματα, υπηρεσίες ή εγκαταστάσεις πρέπει να γίνεται μια φορά κάθε τρεις μήνες.

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Διαδικασίες 005: Έλεγχοι πρόσβασης στις εγκαταστάσεις

1. Επισκόπηση

Η διαδικασία καθορίζει τον τρόπο με τον οποίο θα γίνεται η πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού.

2. Σκοπός

Η διαδικασία αυτή έχει ως σκοπό να καθορίσει τον τρόπο με τον οποίο θα γίνεται η πρόσβασης του προσωπικού στις εγκαταστάσεις του οργανισμού, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.11.1.3

3. Πεδίο Εφαρμογής

Αυτή την διαδικασία εφαρμόζεται από τους:

- Υπεύθυνο Φυσικής Ασφάλειας

4. Διαδικασίες

Όλες οι παρακάτω διαδικασίες θα καταγράφονται από τα συστήματα εισόδου (fingerprint reader, smart card readers), αλλά και από το κλειστό κύκλωμα τηλεόρασης και παρακολουθούνται σε πραγματικό χρόνο από τον υπεύθυνο φυσικής ασφάλειας.

4.1 Πρόσβαση προσωπικού (είσοδος)

4.1.1 Χρήση δακτυλικών αποτυπωμάτων για άνοιγμα της κεντρικής εισόδου.

4.2 Πρόσβαση προσωπικού (γραφεία)

4.2.1 Χρήση smart card για άνοιγμα της πόρτας γραφείου.

4.3 Πρόσβαση επισκεπτών

4.3.1 Χρήση κουδουνιού πόρτας
4.3.2 Άνοιγμα της πόρτας από τον υπεύθυνο υποδοχής (reception)
4.3.3 Υπογραφή στο βιβλίο εισόδου επισκεπτών
4.3.4 Ενημέρωση υπεύθυνου φυσικής ασφάλειας
4.3.5 Ανάθεση συνοδού στον επισκέπτη που θα συνοδεύει τον επισκέπτη στις εγκαταστάσεις του οργανισμού. Αν κριθεί αναγκαίο θα πρέπει να υπογράφεται και σύμφωνο εμπιστευτικότητας από τον επισκέπτη.

4.4 Πρόσβαση στον αποθηκευτικό χώρο εγγράφων & μέσων αποθήκευσης

Για την πρόσβαση στον αποθηκευτικό χώρο εγγράφων & μέσων αποθήκευσης απαιτούνται δυο άτομα. Το ένα άτομο πρέπει να είναι από την Διοίκηση και ένα ακόμα εξουσιοδοτημένο άτομο. Ο χώρος είναι διαμορφωμένος με τέτοιο τρόπο ώστε να πρέπει να ανοίξουν δυο πόρτες (μια από κάθε άτομο) με την χρήση smart card (Σχεδιασμός 002) [36].

Τα εξουσιοδοτημένα άτομα (πολιτική 008) είναι:

- Διευθυντής Ασφάλειας Πληροφοριών
- Διευθυντής Διαχείρισης Εγκαταστάσεων
- Υπεύθυνος Φυσικής Ασφάλειας

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Διαδικασία 006: Διαχείριση κινδύνων

1. Επισκόπηση

Η διαδικασία καθορίζει τον τρόπο με τον οποίο θα γίνεται η διαχείριση κινδύνων.

2. Σκοπός

Η διαδικασία αυτή έχει ως σκοπό να καθορίσει τον τρόπο με τον οποίο θα γίνεται η διαχείριση κινδύνων, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.12.6.1

3. Πεδίο Εφαρμογής

Αυτή την διαδικασία εφαρμόζεται από τους:

- Διευθυντή Ασφάλειας Πληροφοριών

4. Διαδικασία

4.1 Καταγραφή περιουσιακού στοιχείου
4.2 Ορισμός ιδιοκτήτη περιουσιακού στοιχείου
4.3 Αξιολόγηση κινδύνων (ευπάθειες, κίνδυνοι, επιπτώσεις, πιθανότητα εμφάνισης, αξιολόγηση κινδύνων)
4.4 Καθορισμός κριτηρίου αποδοχής κινδύνου
4.5 Αντιμετώπιση Κινδύνων. Για κάθε ευπάθεια (βήμα 4.3) εφαρμόζουμε ελέγχους από το Παράρτημα Α του προτύπου (ή άλλων), για την ελαχιστοποίηση του ρίσκου. Η εφαρμογή των ελέγχων γίνεται συνήθως με την δημιουργία πολιτικών ασφαλείας και διαδικασιών.
4.6 Καθορισμός ημερομηνίας εφαρμογής και τήρηση των πολιτικών και διαδικασιών από τους χρήστες.
4.7 Ενημέρωση της δήλωσης εφαρμοσιμότητας (SoA)

Τα κριτήρια που θέσαμε για την αξιολόγηση των κινδύνων είναι:

Κριτήρια Κινδύνου	Περιγραφή
Κριτήριο Επίπτωσης	Κλίμακα: 1-10 (1 – Μικρή Επίπτωση, 10 – Μεγάλη Επίπτωση). Θα οριστεί βάση της ζημιάς που μπορεί να προκαλέσει στον οργανισμό (οικονομική, νομική, φήμης, κτλ.).
Πιθανότητα Εμφάνισης	Κλίμακα: 1-10 (1 – Μικρή Πιθανότητα, 10 – Μεγάλη Πιθανότητα). Θα οριστεί βάση την κρίση και την εμπειρία μας.
Κριτήριο Αξιολόγησης	Κίνδυνος = Επίπτωση * Πιθανότητα Εμφάνισης.
Κριτήριο Αποδοχής	Κίνδυνος <= 60
Κλίμακα	1-49 Χαμηλός, 50-69 Μέτριος, 70-100 Υψηλός

Πρέπει να ακολουθείται η παραπάνω διαδικασία για κάθε περιουσιακό στοιχείο που έχει αποκτηθεί από τον οργανισμό. Για νέα περιουσιακά στοιχεία η διαδικασία πρέπει να

εφαρμόζεται πριν την διάθεσή τους στους τελικούς χρήστες (ιδιοκτήτες). Επίσης, τεχνικές πληροφορίες σχετικά με την ασφάλεια και τις ευπάθειες του περιουσιακού στοιχείου πρέπει να μελετώνται πριν την απόκτηση του.

Η ανασκόπηση της διαχείρισης κινδύνων πρέπει να γίνεται κάθε 3 μήνες ή όποτε προκύψει ανάγκη για ενημέρωσή του.

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Διαδικασία 007: Συνεργασία μεταξύ πρακτορείων

1. Επισκόπηση

Η διαδικασία καθορίζει τον τρόπο με τον οποίο θα γίνεται η συνεργασία μεταξύ πρακτορείων.

2. Σκοπός

Η διαδικασία αυτή έχει ως σκοπό να καθορίσει τον τρόπο με τον οποίο θα γίνεται η συνεργασία μεταξύ πρακτορείων, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α:

3. Πεδίο Εφαρμογής

Αυτή την διαδικασία εφαρμόζεται από τις διοικήσεις των οργανισμών.

4. Διαδικασία

4.1 Υπογραφή συμφώνου εμπιστευτικότητας και από τα δυο μέρη (NDA 001)
4.2 Υποβολή της σχετικής αίτησης από το άλλο πρακτορείο (Φόρμα 001)
4.3 Ανάλυση στοιχείων της αίτησης. Αν δεν εγκριθεί η αίτηση τότε η διαδικασία σταματά σε αυτό το σημείο και πρέπει να επαναληφθεί η διαδικασία από το βήμα 4.2.
4.4 Αρχική αξιολόγηση πρακτορείου (Αρχείο Καταγραφής 001)
4.5 Υπογραφή συμφωνίας μεταξύ των δυο πρακτορείων (Συμβόλαιο 002)
4.6 Τήρηση της συμφωνίας και από τα δυο μέρη

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Διαδικασία 008: Κύκλος ζωής λογισμικού

1. Επισκόπηση

Η διαδικασία καθορίζει τον τρόπο με τον οποίο θα γίνεται η ανάπτυξη λογισμικού και ο κύκλος ζωής του.

2. Σκοπός

Η διαδικασία αυτή έχει ως σκοπό να καθορίσει τον τρόπο με τον οποίο θα γίνεται η ανάπτυξη λογισμικού, ο κύκλος ζωής του.

Έλεγχοι από το Παράρτημα Α:

3. Πεδίο Εφαρμογής

Αυτή την διαδικασία εφαρμόζεται από τους προγραμματιστές του οργανισμού

4. Διαδικασία

Οι προγραμματιστές του οργανισμού πρέπει να ακολουθούν την παρακάτω διαδικασία για την ανάπτυξη λογισμικού:

4.1 **Σχεδιασμός**:

- Καθορισμός απαιτήσεων της εφαρμογής.
- Σχεδιασμός της εφαρμογής (αρχιτεκτονική, ροή δεδομένων, περιπτώσεις χρήσης, γραφικό περιβάλλον, κτλ.)
- Διαχείριση των κινδύνων της εφαρμογής.

4.2 **Υλοποίηση**: Υλοποίηση (ή αναβάθμιση) της εφαρμογής βάση του σχεδιασμού (βήμα 4.1) και παραγωγή του πηγαίου κώδικα και των εκτελέσιμων αχρείων.

4.3 **Έλεγχος**: Γίνεται έλεγχος της εφαρμογής στο περιβάλλον ελέγχου (Testing Hosts) και αποσφαλμάτωση. Σε αυτό το βήμα εκτός από τον έλεγχο του πηγαίου κώδικα (βήμα 4.2) ελέγχετε ο αρχικός σχεδιασμός (βήμα 4.1) καθώς επίσης και η ποιότητα του κώδικα.

4.4 **Εκτέλεση**: Ανάπτυξη της εφαρμογής και εκτέλεσή της στο περιβάλλον παραγωγής (Production Hosts).

Για κάθε αλλαγή που πρέπει να γίνει στην εφαρμογή ακολουθούνται τα βήματα από την αρχή. Για κάθε βήμα της διαδικασίας πρέπει να υπάρχουν τεκμηριωμένες πληροφορίες όπως:

- Απαιτήσεις της εφαρμογής / Σχεδιασμός
- Διαχείριση Κινδύνων εφαρμογής
- Πηγαίος κώδικας
- Αποτελέσματα Ελέγχων/ Αποσφαλμάτωσης
- Αρχεία καταγραφής συμβάντων

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Διαδικασία 009: Αναφορά γεγονότος / περιστατικού ασφαλείας

1. Επισκόπηση

Η διαδικασία καθορίζει τον τρόπο με τον οποίο θα γίνεται η αναφορά γεγονότων και περιστατικών ασφαλείας από το προσωπικό.

2. Σκοπός

Η διαδικασία αυτή έχει ως σκοπό να καθορίσει τον τρόπο με τον οποίο θα γίνεται η αναφορά γεγονότων και περιστατικών ασφαλείας από το προσωπικό, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013 και GDPR.

Έλεγχοι από το Παράρτημα Α: 16.1.1, Α.16.1.2, Α.16.1.3, Α.16.1.4, Α.16.1.5, Α.16.1.6, Α.16.1.7

3. Πεδίο Εφαρμογής

Αυτή την διαδικασία εφαρμόζεται από όλο το προσωπικό του οργανισμού

4. Διαδικασία

Όλο το προσωπικό είναι υποχρεωμένο να αναφέρει τα γεγονότα και περιστατικά ασφαλείας ή αδυναμίες συστημάτων σχετικές με την ασφάλεια στον διευθυντή ασφαλείας πληροφοριών.

Μόλις αντιληφθεί ένα τέτοιο περιστατικό πρέπει να:

4.1 Αναφέρει το συντομότερο δυνατό το περιστατικό στον διευθυντή ασφάλειας πληροφοριών.
4.2 Στην περίπτωση που είναι εφικτό, το άτομο που αντιλαμβάνεται το περιστατικό πρέπει να προχωρήσει στην συλλογή αποδεικτικών στοιχείων που να αποδεικνύει την ύπαρξη του περιστατικού και να τα αποστείλει με **ασφαλή** τρόπο στον διευθυντή ασφαλείας πληροφοριών.
4.3 Ο διευθυντής ασφάλειας πληροφοριών, αφού καταγράψει το γεγονός ή το περιστατικό (Αρχείο Καταγραφής 005) θα προχωρήσει στην συλλογή επιπρόσθετων αποδεικτικών στοιχείων (αν δεν υπάρχουν αρκετά).
4.4 Αφού γίνει ο κατάλληλος συντονισμός με το κατάλληλο προσωπικό, θα γίνει προσπάθεια λήψης διορθωτικών ενεργειών και αξιολόγησης της επίπτωσης που είχε στον οργανισμό το περιστατικό.
4.5 Σε περίπτωση που υπήρξε παράνομη δραστηριότητα ή διαρροή δεδομένων προσωπικού χαρακτήρα, τότε πρέπει να γίνει αναφορά του περιστατικού στις αρχές του κράτους.

Πρέπει να γίνει παρακολούθηση της υλοποίησης των διορθωτικών ενεργειών (βάση του πλάνου).

Όπου χρειαστεί πρέπει να ληφθούν πειθαρχικά μέτρα (Διαδικασία 002), ενώ η γνώση που αποκτήθηκε από κάθε περιστατικό ασφαλείας πρέπει να χρησιμοποιηθεί με τέτοιο τρόπο ώστε να μην επαναληφθεί στο μέλλον.

Αν το περιστατικό αφορά κενό ασφαλείας σε υπηρεσία που παρέχεται από τρίτους, τότε ο διευθυντής ασφάλειας πληροφοριών πρέπει να το αναφέρει στον προμηθευτή και να

παρακολουθεί την όλη διαδικασία ώστε να τηρηθεί η συμφωνία επιπέδου υπηρεσίας (SLA).

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Διαδικασία 010: Εσωτερική επιθεώρηση

1. Επισκόπηση

Η διαδικασία καθορίζει τον τρόπο με τον οποίο θα γίνεται η εσωτερική επιθεώρηση του ΣΔΑΠ.

2. Σκοπός

Η διαδικασία αυτή έχει ως σκοπό να καθορίσει τον τρόπο με τον οποίο θα γίνεται η εσωτερική επιθεώρηση του ΣΔΑΠ, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013 και GDPR.

Έλεγχοι από το Παράρτημα Α: 18.2.2

3. Πεδίο Εφαρμογής

Αυτή την διαδικασία εφαρμόζεται από τον εσωτερικό ελεγκτή.

4. Διαδικασία

4.1 Έλεγχος συμμόρφωσης με τις πολιτικές ασφάλειας, διαδικασίες και σχεδιασμούς. Αυτό πρέπει να γίνεται μέσω συνέντευξης όπου θα γίνεται παρουσίαση αποδεικτικών στοιχείων (δειγματοληπτικά) από το άτομο που επιθεωρείται.
4.2 Σε περιπτώσεις μη συμμόρφωσης θα πρέπει άμεσα να ληφθούν διορθωτικές ενέργειες.
4.2 Σύνταξη αναλυτικής αναφοράς με τα ευρήματα (Φόρμα 002).
4.3 Για κάθε μη συμμόρφωση πρέπει να γίνεται άμεσα λήψη διορθωτικών ενεργειών (με αποδεικτικά στοιχεία).
4.4 Συζήτηση των αποτελεσμάτων με την διοίκηση. Για σοβαρά περιστατικά μη συμμορφώσεων, ίσος κριθεί αναγκαίο να ληφθούν πειθαρχικές ενέργειες.

Σε περίπτωση που βρεθούν μη συμμορφώσεις πρέπει να γίνει παρακολούθηση υλοποίησης τους (βάση του πλάνου).

Η εσωτερική επιθεώρηση πρέπει να γίνεται κάθε 6 μήνες.

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Διαδικασία 011: Επικοινωνία

1. Επισκόπηση

Η διαδικασία καθορίζει τον τρόπο με τον οποίο θα γίνεται η επικοινωνία με το προσωπικό και τους εξωτερικούς συνεργάτες του οργανισμού.

2. Σκοπός

Η διαδικασία αυτή έχει ως σκοπό να καθορίσει τον τρόπο με τον οποίο θα γίνεται η επικοινωνία με το προσωπικό και τους εξωτερικούς συνεργάτες του οργανισμού, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013 και GDPR.

Έλεγχοι από το Παράρτημα Α:

3. Πεδίο Εφαρμογής

Αυτή την διαδικασία εφαρμόζεται από τους:

- Διευθυντή Ασφάλειας Πληροφοριών
- Διευθυντή Ανθρώπινου Δυναμικού
- Διευθυντή Διαχείρισης Εγκαταστάσεων

4. Διαδικασία

Μόλις προκύψει ανάγκη για επικοινωνία πρέπει:

4.1 Να καθοριστεί το περιεχόμενο της επικοινωνίας.
4.2 Να καθοριστεί πότε θα πραγματοποιηθεί η επικοινωνία.
4.3 Να καθοριστεί το καταλληλότερο κανάλι επικοινωνίας (e-mail, τηλέφωνο, SMS, συναγερμός, κτλ.)
4.4 Διενέργεια της επικοινωνίας / Επιβεβαίωση λήψης του μνήματος
4.5 Ενημέρωση του αρχείου καταγραφής 008

Το περιεχόμενο της επικοινωνίας μπορεί να είναι:

- Οι πολιτικές ασφαλείας και οι διαδικασίες ή οι ενημερωμένες εκδόσεις τους.
- Νομοθεσία (π.χ. Εφαρμογή του GDPR)
- Γνώση σχετικά με νέες απειλές και τρόπους αντιμετώπισης τους.
- Οι στόχοι ασφαλείας.
- Περιπτώσεις έκτακτης ανάγκης (π.χ. άσκηση ετοιμότητας).
- Ενημέρωση για εκπαίδευση/εκδηλώσεις σχετικές με την ασφάλεια πληροφοριών.
- Αλλαγές που έγιναν στο ΣΔΑΠ.

5. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Διαδικασία 012: Αλλαγές στο ΣΔΑΠ

9. Επισκόπηση

Η διαδικασία καθορίζει τον τρόπο με τον οποίο θα γίνονται οι αλλαγές στο ΣΔΑΠ.

10. Σκοπός

Η διαδικασία αυτή έχει ως σκοπό να καθορίσει τον τρόπο με τον οποίο θα γίνονται οι αλλαγές στο ΣΔΑΠ, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013.

Έλεγχοι από το Παράρτημα Α: Α.12.1.2

11. Πεδίο Εφαρμογής

Αυτή την διαδικασία εφαρμόζεται από όλο το προσωπικό.

12. Διαδικασία

Μόλις προκύψει ανάγκη για αλλαγές στο ΣΔΑΠ πρέπει:

4.1 Να αποσταλεί η σχετική γραπτή αίτηση με e-mail στον διευθυντή ασφάλειας πληροφοριών, αναλύοντας τους λόγους σχετικά με τις αλλαγές που πρέπει να γίνουν. Το e-mail θα πρέπει να έχει θέμα «ISMS Request For Change - <θέμα>».
4.2 Ο διευθυντής ασφάλειας πληροφοριών με την βοήθεια προσωπικού που σχετίζεται με τις αλλαγές, αφού αναλύσει την αίτηση, τους κινδύνους και τις πιθανές επιπτώσεις που θα έχουν στον οργανισμό (π.χ. οικονομικές) θα προχωρήσει στην έγκριση ή όχι των αλλαγών.
4.3 Στην περίπτωση έγκρισης των αλλαγών τότε ο οργανισμός προχωρά με την υλοποίηση τους.

Επιπλέον, πρέπει να διασφαλιστεί ότι θα υπάρχει δυνατότητα εύκολης επαναφοράς στην αρχική κατάσταση σε περίπτωση αποτυχία εφαρμογής της αλλαγής.

13. Συμμόρφωση με την Διαδικασία

Έλεγχος: Η συμμόρφωση με αυτή την διαδικασία θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με την διαδικασία θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

14. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

15. Όροι και Ορισμοί

Όχι

16. Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών

29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Παράρτημα Γ

Σχεδιασμοί

Γ.1 Σχεδιασμοί

Σχεδιασμός 001: Επιχειρησιακή συνέχεια

9. Επισκόπηση

Με τον σχεδιασμό αυτό διασφαλίζεται ότι θα υπάρχει επιχειρησιακή συνέχεια μετά από μια κρίση ή καταστροφή

10. Σκοπός

Ο σκοπός αυτού του σχεδιασμό είναι να διασφαλίσει την επιχειρησιακή συνέχεια μετά από μια κρίση ή καταστροφή, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013

Έλεγχοι από το Παράρτημα Α: Α.17.1.1, Α.17.1.2, Α.17.1.3, Α.17.2.1

11. Πεδίο Εφαρμογής

Αυτός ο σχεδιασμός εφαρμόζεται από τους:

- Διαχειριστή Συστημάτων και Δικτύων
- Διευθυντή Ασφάλειας Πληροφοριών
- Διευθυντή Διαχείρισης Εγκαταστάσεων

12. Σχεδιασμός

Ο οργανισμός έχει λάβει σοβαρά υπόψιν το θέμα της επιχειρησιακής συνέχειας. Για αυτό τον λόγο έχει υλοποιήσει ελέγχους που αφορούν τόσο την φυσική όσο και την ψηφιακή ασφάλεια των περιουσιακών του στοιχείων σε περίπτωση κρίσης ή φυσικής καταστροφής.

Συγκεκριμένα:

- Οι κτιριακές εγκαταστάσεις βρίσκονται σε περιοχή με πολύ χαμηλή εγκληματικότητα όπου γίνονται συχνές περιπολίες από την αστυνομία της περιοχής.

- Οι εγκαταστάσεις έχουν αντισεισμικό σχεδιασμό και επιλεχθήκαν ώστε να βρίσκονται σε όροφο για να υπάρχει μειωμένη πιθανότητα πλημύρας.

- Σε όλα τα συστήματα έχουν εγκατασταθεί UPS για αδιάληπτή παροχή ρεύματος σε περίπτωση διακοπής ηλεκτρικού ρεύματος.

- Η πρόσβαση στο διαδίκτυο γίνεται από δυο εταιρίες παροχής υπηρεσιών διαδικτύου (ISP) [35].

- Όλα τα αντικείμενα (Workstations, Servers, ράφια, βιβλιοθήκες, κτλ.) είναι στερεωμένα στους τείχους ώστε να αποφευχθούν οι πτώσεις ακόμα και σε περίπτωση ισχυρής σεισμικής δόνησης.

- Η συντήρηση του εξοπλισμού γίνεται με βάση τις επίσημες οδηγίες του κατασκευαστή.

- Έγινε εγκατάσταση ισχυρού αντικλεπτικού, αντιπλημμυρικού και αντιπυρικού συστήματος.

- Έγινε εγκατάσταση κλειστού κυκλώματος τηλεόρασης (CCTV).

- Έγινε εγκατάσταση ισχυρών κλειδαριών με σύστημα σάρωσής δακτυλικών αποτυπωμάτων (είσοδος) και smart cards (γραφεία).

- Στα γραφεία όπου υπάρχουν οι Servers (Server Room) και στον αποθηκευτικός χώρο εγγράφων & μέσων αποθήκευσης (Safe Storage Room) δεν υπάρχουν παράθυρα, ώστε να μειωθεί περισσότερο η πιθανότητα κακόβουλης ενέργειας.

- Στον αποθηκευτικός χώρο εγγράφων & μέσων αποθήκευσης (Safe Storage Room) υπάρχει σύστημα διπλής εισόδου.

- Τηρούνται αντίγραφα ασφαλείας όλων των σημαντικών εγγράφων (NDAs, contracts, κτλ.) και ψηφιακών αρχείων όλων των συστημάτων του οργανισμού κάθε μια ώρα. Τα αντίγραφα ασφάλειας τηρούνται σε NAS Server με συστοιχίες δίσκων σε RAID 6 (Redundant Array of Independent Disks).

- Διοργανώνονται από τον οργανισμό εκπαιδευτικά σεμινάρια ώστε να υπάρχει ετοιμότητα από όλο το προσωπικό.

- Υπάρχουν καταγεγραμμένες διαδικασίες (βάση της εκπαίδευσης) ώστε όλο το προσωπικό να γνωρίζει πώς πρέπει να ενεργήσει σε περίπτωση κρίσης ή καταστροφής.

- Εκτελούνται ασκήσεις ετοιμότητας (σενάρια) σε τυχαίους χρόνους ώστε να εξακριβωθεί ο βαθμός ετοιμότητας του οργανισμού μετά από μια κρίση ή καταστροφή.

- Γίνεται τακτική επικοινωνία από τον διευθυντή ασφάλειας πληροφοριών και τον διευθυντή διαχείρισης εγκαταστάσεων με το προσωπικό, για θέματα που αφορούν την ασφάλεια των δεδομένων ή την φυσική ασφάλεια (π.χ. προστασία από νέες απειλές).

<u>Μελλοντικά Σχέδια:</u>

- Δημιουργία μιας βάσης δεδομένων όπου θα καταγράφονται οι διαδικασίες, οι πολιτικές και η γνώση (knowledge base) που αποκτήθηκαν από την λειτουργία του οργανισμού. Ο λόγος δημιουργίας της βάσης είναι για την άμεση ανάκτηση των συγκεκριμένων πληροφοριών από το προσωπικό αλλά και για την ομαλή προσαρμογή στον οργανισμό νέου προσωπικού. Επιπλέον η βάση αυτή θα χρησιμοποιείται σε περιπτώσεις ανάγκης για έκτακτη αντικατάσταση προσωπικού (π.χ. σε περίπτωση άδειας, ασθένειας, άμεσου τερματισμού εργασίας, κτλ.) [33].

- Ο οργανισμός μελετά το ενδεχόμενο δημιουργίας εναλλακτικής τοποθεσίας (recovery cold site) όπου θα τηρούνται αντίγραφα ασφαλείας των ψηφιακών αρχείων όσο και των εγγράφων (πιστοποιημένα αντίγραφα).

- Υλοποίηση και πιστοποίηση συστήματος διαχείρισης επιχειρησιακής συνέχειας (BCMS), βάση του διεθνούς προτύπου ISO 22301.

- Εγκατάσταση ηλεκτρογεννήτριας για αδιάληπτη ηλεκτρική ενέργεια, σε περίπτωση διακοπής ηλεκτρικού ρεύματος [35].

13. Συμμόρφωση με την Σχεδιασμό

Έλεγχος: Η συμμόρφωση με αυτό τον σχεδιασμό θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με αυτό τον σχεδιασμό θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

14. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

15. Όροι και Ορισμοί

Όχι

16. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Σχεδιασμός 002: Φυσική και περιβαλλοντική ασφάλεια

1. **Επισκόπηση**

   Με τον σχεδιασμό αυτό διασφαλίζεται ότι θα υπάρχει φυσική και περιβαλλοντική ασφάλεια στον οργανισμό.

2. **Σκοπός**

   Ο σκοπός αυτού του σχεδιασμό είναι να διασφαλίσει την φυσική και περιβαλλοντική ασφάλεια στον οργανισμό, καθώς επίσης η συμμόρφωση με το πρότυπο ISO 27001:2013

   Έλεγχοι από το Παράρτημα Α: A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6

3. **Πεδίο Εφαρμογής**

   Αυτός ο σχεδιασμός εφαρμόζεται από τον υπεύθυνο φυσικής ασφάλειας.

4. **Σχεδιασμός**

   Ο οργανισμός έχει λάβει σοβαρά υπόψιν το θέμα της φυσικής και περιβαλλοντικής ασφάλειας. Για αυτό τον λόγο έχει υλοποιήσει ελέγχους που αφορούν την φυσική ασφάλεια των περιουσιακών στοιχείων του ώστε να διασφαλιστεί την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων ή άλλων εγκληματικών πράξεων.

   Ακολουθούν εικόνες που δείχνου τους ελέγχους φυσικής ασφάλειας που εφαρμόστηκαν.

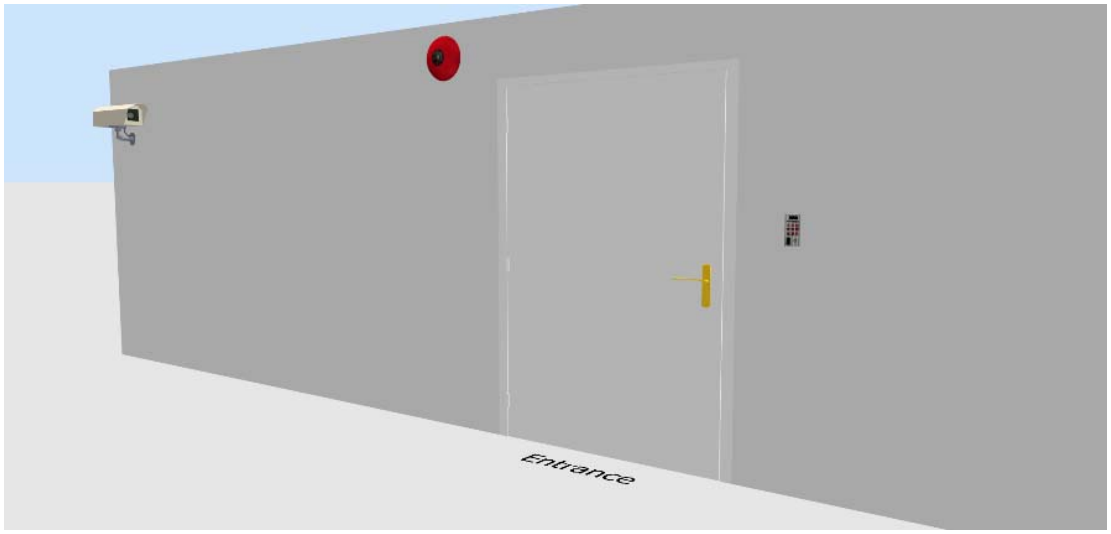
   Κάτοψη (Εικόνα Γ.1):

Εικόνα Γ.1: Οι κτηριακές εγκαταστάσεις (κάτοψη)

   Είσοδος:

   - Προειδοποιητική πινακίδα ύπαρξης κλειστού κυκλώματος τηλεόρασης (CCTV) (Εικόνα Γ.7)
   - Προειδοποιητική πινακίδα λήψης φωτογραφιών και βίντεο (Εικόνα Γ.8)
   - Σάρωση δακτυλικών αποτυπωμάτων (Εικόνα Γ.2)

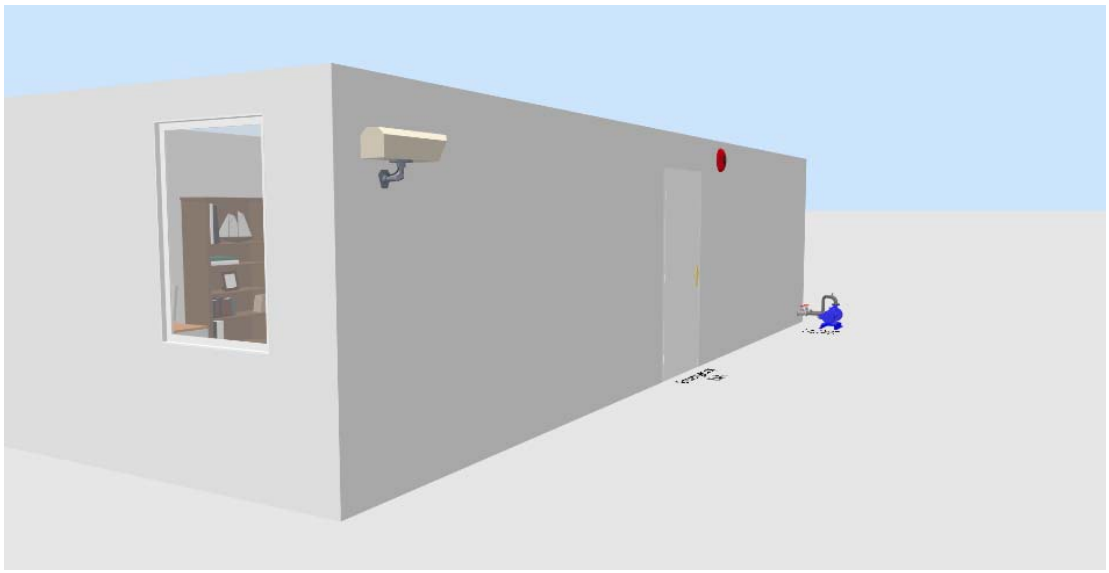
- CCTV (Εικόνα Γ.2)
- Εξωτερική Σειρήνα #1 (Εικόνα Γ.2)



Εικόνα Γ.2: Οι κτηριακές εγκαταστάσεις (είσοδος)

Έξοδος κινδύνου:

- Αντιπλημμυρική αντλία (Εικόνα Γ.3)
- Εξωτερική Σειρήνα #2 (Εικόνα Γ.3)

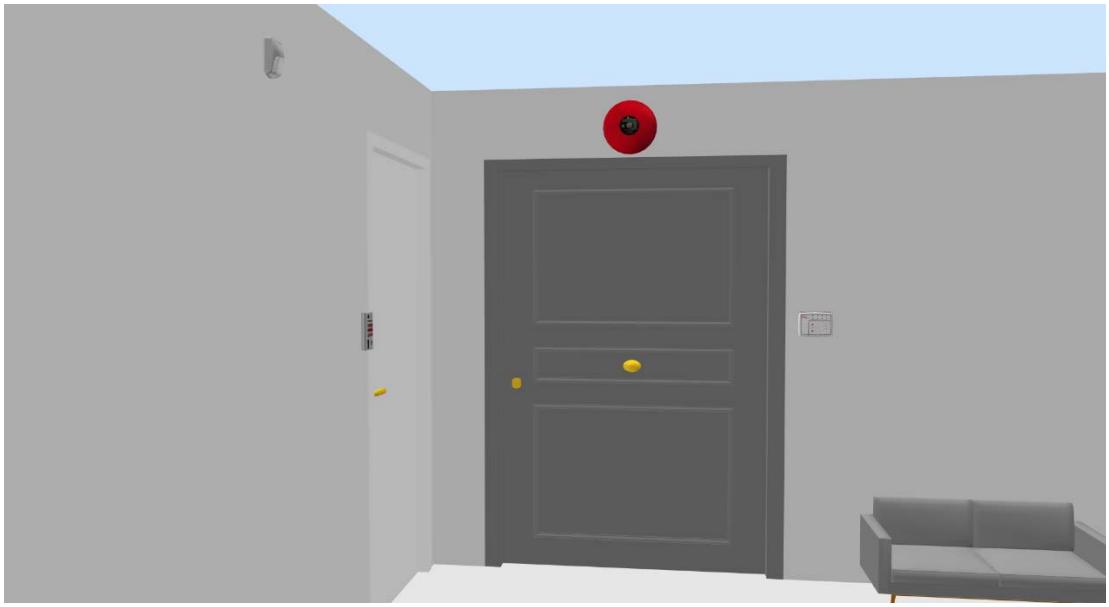


Εικόνα Γ.3: Οι κτηριακές εγκαταστάσεις (έξοδος κινδύνου)

Εσωτερικό:

- Προειδοποιητική πινακίδα ύπαρξης κλειστού κυκλώματος τηλεόρασης (CCTV) (Εικόνα Γ.7)
- Προειδοποιητική πινακίδα λήψης φωτογραφιών και βίντεο (Εικόνα Γ.8)
- Αισθητήρες συναγερμού (Εικόνα Γ.4)
- Εσωτερική Σειρήνα (Εικόνα Γ.4)
- Έλεγχος πρόσβασης γραφείων (Εικόνα Γ.5)
- CCTV (Εικόνα Γ.5)
- Συναγερμός Πυρκαγιάς (Εικόνα Γ.5)

- Πυροσβεστήρες (Εικόνα Γ.6)



Εικόνα Γ.4: Οι κτηριακές εγκαταστάσεις (εσωτερική είσοδος)

Εικόνα Γ.5: Οι κτηριακές εγκαταστάσεις (είσοδοι γραφείων)

Εικόνα Γ.6: Οι κτηριακές εγκαταστάσεις (υποδοχή)

Εικόνα Γ.7: Προειδοποιητική πινακίδα CCTV [28]

Εικόνα Γ.8: Προειδοποιητική πινακίδα λήψης φωτογραφιών και βίντεο [29]

5. Συμμόρφωση με την Σχεδιασμό

Έλεγχος: Η συμμόρφωση με αυτό τον σχεδιασμό θα ελέγχεται μέσω της εσωτερικής επιθεώρησης ή με τυχαίους δειγματοληπτικούς ελέγχους.

Εξαιρέσεις: Όχι

Μη συμμόρφωση: Η μη συμμόρφωση με τον σχεδιασμό θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.

6. Σχετικά Πρότυπα, Πολιτικές και διαδικασίες

Όχι

7. Όροι και Ορισμοί

Όχι

8. Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Παράρτημα Δ

Αρχεία καταγραφής

Δ.1 Αρχείο Καταγραφής 001 - Αξιολόγηση πρακτορείων Mobile Agents

Αξιολόγηση Πρακτορείων Mobile Agents							
Όνομα Πρακτορείου	**Εφαρμογή ΣΔΑΠ;**	**Επιθεώρηση ΣΔΑΠ από τον Οργανισμό XYZ;**	**Επιθεώρηση του κώδικα των mobile agents από τον Οργανισμό XYZ;**	**Διαπιστευμένη Πιστοποίηση ΣΔΑΠ;**	**Υπογραφή NDA;**	**Σοβαρά Περιστατικά Ασφαλείας;**	**Βαθμός (MAX=5)**

Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Δ.2 Αρχείο Καταγραφής 002 - βιβλίο επισκεπτών

Βιβλίο Επισκεπτών					
Όνομα/Επίθετο	**Αρ. Ταυτότητας**	**Ημερομηνία/ Ώρα Εισόδου**	**Λόγος Επίσκεψης**	**Συνοδός**	**Ημερομηνία/ Ώρα Εξόδου**

Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Δ.3 Αρχείο Καταγραφής 003 – Εξουσιοδοτημένοι παραλήπτες περιουσιακών στοιχείων

Εξουσιοδοτημένοι παραλήπτες περιουσιακών στοιχείων		
Περιουσιακό Στοιχείο	**Διαβάθμιση**	**Παραλήπτες**

Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Δ.4 Αρχείο Καταγραφής 004 – Εξουσιοδοτημένο λογισμικό

Εξουσιοδοτημένο Λογισμικό	
Εφαρμογή	**Κριτίρια Επιλογής**

Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Δ.5 Αρχείο Καταγραφής 005 – Γεγονότα και Περιστατικά ασφαλείας

Γεγονότα και Περιστατικά ασφαλείας				
Ημερομηνία/Ώρα	**Περιγραφή γεγονότος / περιστατικού**	**Σοβαρότητα / Επιπτώσεις**	**Διορθωτικές Ενέργειες**	**Πλάνο υλοποίησης διορθωτικών ενεργειών**

Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Δ.6 Αρχείο Καταγραφής 006 – Επαγγελματική επάρκεια προσωπικού

Επαγγελματική Επάρκεια Προσωπικού			
Όνομα/ Επίθετο	**Ρόλος**	**Τίτλος Πτυχίου/Σεμιναρίου**	**Σχέση τίτλου με την ασφάλεια πληροφοριών**

Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Δ.7 Αρχείο Καταγραφής 007 – Εκπαίδευση προσωπικού

Εκπαίδευση Προσωπικού			
Τίτλος εκπαίδευσης	**Ημερομηνία διεξαγωγής**	**Τόπος διεξαγωγής**	**Συμμετέχοντες**
ESET Cybersecurity Awareness Training	28/4/2019	Online [www.eset.com/us/cybertraining]	Όλο το προσωπικό

Ιστορικό Αναθεώρησης

Ημερομηνία	Υπεύθυνος	Περίληψη Αλλαγών
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Δ.8 Αρχείο Καταγραφής 008 – Επικοινωνία

	Επικοινωνία				
Υπεύθυνος Επικοινωνίας	**Περιεχόμενο**	**Ημερομηνία διεξαγωγής**	**Τόπος διεξαγωγής**	**Τρόπος διεξαγωγής**	**Συμμετέχοντες**

Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Δ.8 Αρχείο Καταγραφής 009 – Μη συμμορφώσεις (μετά από δειγματοληπτικό έλεγχο)

Μη Συμμορφώσεις (μετά από δειγματοληπτικό έλεγχο)				
Ημερομηνία/Ώρα	**Μη Συμμόρφωση**	**Σοβαρότητα Μη Συμμόρφωσης**	**Διορθωτικές Ενέργειες**	**Πλάνο υλοποίησης διορθωτικών ενεργειών**

Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Παράρτημα Ε

Φόρμες

Ε.1 Φόρμες

Φόρμα 001 - Αίτηση για εκτέλεση mobile agent στην πλατφόρμα του Οργανισμού XYZ

1. Στοιχεία Εταιρίας:

Όνομα Εταιρίας	
Έδρα Εταιρίας	
Εκπρόσωπος Εταιρίας	
Στοιχεία επικοινωνίας	
Προηγήθηκε υπογραφή συμβολαίου (Συμβόλαιο 002 - Συμβόλαιο Between Agencies) με τον οργανισμό XYZ	Ναι: ☐ Όχι: ☐

2. Στοιχεία Mobile Agent:

Mobile Agent Name	CodeBase	Σκοπός Mobile Agent	Πόροι / δικαιώματα που απαιτούνται	Αιτιολογία
mytest	file:/C:/aglets/public/MSc	Συλλογή κρυπτογραφημένων δεδομένων	Διάβασμα του αρχείου /../enc_data.txt	Διάβασμα των κρυπτογραφημένων δεδομένων
			Διάβασμα του αρχείου /../data_sig.txt	Διάβασμα της ψηφιακής υπογραφής για έλεγχο ακεραιότητας των δεδομένων
			Δικαίωμα για dispatch	Για επιστροφή του agent

3. Διαδρομή Mobile Agent:

Host B -> Host A -> Host B

Ο αιτών:	Εγκρίθηκε από:
Όνομα: ……	Όνομα: ……
Ιδιότητα: ……..	Ιδιότητα: ……..
Ημερομηνία: ……/……/…… [ηη/μμ/χχχχ]	Ημερομηνία: ……/……/…… [ηη/μμ/χχχχ]
Υπογραφή:……..	Υπογραφή:……..

Φόρμα 002 - Αναφορά εσωτερικής επιθεώρησης

Σκοπός της εσωτερικής επιθεώρησης:

Συμμόρφωση με το Πρότυπο ISO 27001:

Παράγραφος	Ευρήματα/ Μη Συμμορφώσεις	Διορθωτικές Ενέργειες	Πλάνο υλοποίησης διορθωτικών ενεργειών
4.1 – Κατανόηση του οργανισμού και του πλαισίου λειτουργίας του			
4.2 – Κατανόηση των αναγκών και προσδοκιών των ενδιαφερόμενων μερών			
4.3 – Καθορισμός πεδίου εφαρμογής του ΣΔΑΠ			
4.4 – Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών			
5.1 – Ηγεσία και Δέσμευση			
5.2 – Πολιτική Ασφαλείας			
5.3 – Οργανωτικοί ρόλοι, ευθύνες και εξουσίες			
6.1 – Ενέργειες αντιμετώπισης κινδύνων και αξιοποίησης ευκαιριών			
6.2 – Στόχοι ασφάλειας πληροφοριών και σχεδιασμός για επίτευξή τους			
7.1 - Πόροι			
7.2 – Επαγγελματική επάρκεια			
7.3 – Ευαισθητοποίηση			
7.4 - Επικοινωνία			
7.5 – Τεκμηριωμένες πληροφορίες			
8.1 – Σχεδιασμός, λειτουργία και έλεγχος των διεργασιών			
8.2 – Αξιολόγηση κινδύνου			
8.3 – Ενέργειες μετριασμού κινδύνου			
9.1 – Παρακολούθηση, μέτρηση ανάλυση και αξιολόγηση			
9.2 – Εσωτερική επιθεώρηση			
9.3 – Ανασκόπηση διοίκησης			
10.1 – Μη συμμόρφωση και διορθωτικές ενέργειες			
10.2 – Συνεχής βελτίωση			

Συμμόρφωση με Πολιτικές, Διαδικασίες, Σχεδιασμούς, Αρχεία Καταγράφων, Φόρμες:

Πολιτική/Διαδικασία/Σχεδιασμός/ Αρχείο Καταγράφων/Φόρμα	Υπεύθυνος	Ευρήματα/ Μη Συμμορφώσεις	Διορθωτικές Ενέργειες	Πλάνο υλοποίησης διορθωτικών ενεργειών
Πολιτική 001: Επικοινωνία με τις Αρχές και με Ομάδες ειδικών ενδιαφερόντων				
Πολιτική 002: Ασφάλεια Πληροφοριών στην Διαχείριση Έργων				
Πολιτική 003: Ασφάλεια Κινητών Συσκευών				
Πολιτική 004: Ασφάλεια Ανθρώπινου Δυναμικού				
Πολιτική 005: Διαβάθμιση των πληροφοριών				
Πολιτική 006: Αποδεκτή χρήση των περιουσιακών στοιχείων				
Πολιτική 007: Συμμόρφωση με τις απαιτήσεις της νομοθεσίας και των συμβολαίων				
Πολιτική 008: Απαιτήσεις του οργανισμού για τον έλεγχο πρόσβασης				
Πολιτική 009: Σύστημα Διαχείρισης Κωδικών Πρόσβασης				
Πολιτική 010: Χρήση Κρυπτογράφησης				
Πολιτική 011: Καθαρό γραφείο/Καθαρή οθόνη				

Πολιτική 012: Τήρηση αρχείων καταγραφής συμβάντων				
Πολιτική 013: Προφίλ Ασφάλειας Υπολογιστικών Συστημάτων				
Πολιτική 014: Απαιτήσεις Ελέγχων Επιθεώρησης Υπολογιστικών Συστημάτων				
Πολιτική 015: Ασφάλεια Δικτύου				
Πολιτική 016: Ασφάλεια στην ανάπτυξη λογισμικού				
Πολιτική 017: Οι Σχέσεις με τους Προμηθευτές				
Πολιτική 018: Τυχαίοι δειγματοληπτικοί έλεγχοι				
Διαδικασία 001: Καθορισμός Πολιτικών Ασφάλειας Πληροφοριών				
Διαδικασία 002: Πειθαρχική διαδικασία				
Διαδικασία 003: Χειρισμός Περιουσιακών στοιχείων				
Διαδικασίες 004: Διαχείριση πρόσβασης χρηστών				
Διαδικασίες 005: Έλεγχοι πρόσβασης στις εγκαταστάσεις				
Διαδικασία 006: Διαχείριση κινδύνων				
Διαδικασία 007: Συνεργασία μεταξύ πρακτορείων				
Διαδικασία 008: Κύκλος Ζωής Λογισμικού				
Διαδικασία 009: Αναφορά Περιστατικού Ασφαλείας				
Διαδικασία 010: Εσωτερική επιθεώρηση				
Διαδικασία 011: Επικοινωνία				
Διαδικασία 012: Αλλαγές στο ΣΔΑΠ				
Σχεδιασμός 001: Επιχειρησιακή Συνέχεια				
Σχεδιασμός 002: Φυσική και Περιβαλλοντική Ασφάλεια				
Αρχείο Καταγραφής 001 - Αξιολόγηση Πρακτορείων Mobile Agents				
Αρχείο Καταγραφής 002 - Βιβλίο Επισκεπτών				
Αρχείο Καταγραφής 003 – Εξουσιοδοτημένοι παραλήπτες περιουσιακών στοιχείων				
Αρχείο Καταγραφής 004 – Εξουσιοδοτημένο Λογισμικό				
Αρχείο Καταγραφής 005 – Γεγονότα και Περιστατικά ασφαλείας				
Αρχείο Καταγραφής 006 – Επαγγελματική Επάρκεια Προσωπικού				
Αρχείο Καταγραφής 007 – Εκπαίδευση Προσωπικού				
Αρχείο Καταγραφής 008 – Επικοινωνία				
Φόρμα 001 - Αίτηση για εκτέλεση mobile agent στην πλατφόρμα του Οργανισμού ΧΥΖ				
Φόρμα 002 - Αναφορά Εσωτερικής Επιθεώρησης				
Φόρμα 003 - Ανασκόπηση διοίκησης				

Σχόλια:

……
……
……
……
……

Διενεργήθηκε από:

Υπογραφή: _____

Ημερομηνία: _____

Εγκρίθηκε από:

Υπογραφή: _____

Ημερομηνία: _____

Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Φόρμα 003 - Ανασκόπηση διοίκησης

Έλαβαν μέρος οι:

……
……
……
……
……
……

Θέματα που συζητήθηκαν:

……
……
……
……
……
……

Ενέργειες που έχουν ληφθεί από την τελευταία ανασκόπηση:

……
……
……
……
……
……

Αλλαγές σε εξωτερικά ή εσωτερικά ζητήματα που σχετίζονται με το ΣΔΑΠ:

……
……
……
……
……
……

Μη συμμορφώσεις με το πρότυπο ISO 27001:2013:

……
……
……
……
……
……

Διορθωτικές ενέργειες που έχουν ληφθεί:

……
……
……
……
……
……

Αποτελέσματα αναλύσεων:

……
……
……
……
……
……

Αποτελέσματα επιθεωρήσεων:

……
……
……
……
……
……

Εκπλήρωση των στόχων:

……
……
……
……
……
……

Η ανατροφοδότηση από τα ενδιαφερόμενα μέρη:

……
……
……
……
……
……

Αποτελέσματα της διαδικασίας της διαχείρισης κινδύνων:

……
……
……
……
……
……

Βελτιώσεις που πρέπει να γίνουν:

……
……
……
……
……
……

Διενεργήθηκε από:

Υπογραφή: _____

Ημερομηνία: _____

Εγκρίθηκε από:

Υπογραφή: _____

Ημερομηνία: _____

Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Παράρτημα Ζ

Συμβόλαια και NDAs

Ζ.1 Συμβόλαια και NDAs

Για την σύνταξη των συμβολαίων και των NDA βασιστήκαμε στα υποδείγματα των Xavier Mertens [20] και κύριου Πέτρου Ραπανάκι [21], αρκετά σημεία προσαρμόστηκαν στις ανάγκες της διατριβής.

NDA 001 - Σύμφωνο Εμπιστευτικότητας

Το παρόν σύμφωνο τίθεται σε ισχύ σήμερα ……/……/……. [ηη/μμ/χχχχ] από και μεταξύ των:

Οργανισμός ΧΥΖ, που εδρεύει στην οδό <διεύθυνση>, Κύπρος και Αριθμό μητρώου <αρ. μητρώου> και εκπροσωπείτε από τον/την κύριο/κυρία <όνομα>, ιδιοκτήτη

Και

Όνομα Εταιρίας	
Έδρα Εταιρίας	
Εκπρόσωπος Εταιρίας	

που παρακάτω θα αναφέρεται ως «συνεργάτης».

Με το παρόν συμβόλαιο, ο συνεργάτης αναγνωρίζει και συμφωνεί ότι:

1. Και τα δυο μέρη υποχρεούνται να τηρούν απόλυτη εχεμύθεια για πληροφορίες που αποκαλύφθηκαν και από τα δυο μέρη κατά την συνεργασία τους.
2. Και τα δυο μέρη δεσμεύονται ότι δεν θα χρησιμοποιήσουν ή θα αποκαλύψουν πληροφορίες ή θα ανακοινώσουν προφορικά ή θα διαρρεύσουν εγγράφως ή με οποιονδήποτε άλλο τρόπο θα διαβιβάσουν ή θα γνωστοποιήσουν προς τρίτους για οποιονδήποτε λόγο ή σκοπό:
    a. Μηνύματα
    b. Κωδικούς πρόσβασης
    c. Εμπορικές πληροφορίες
    d. Άλλες πληροφορίες που βρίσκονται σε έντυπη ή ψηφιακή μορφή
    e. Φόρμουλες
    f. Λογισμικό
    g. Πηγαίο κώδικα λογισμικού / αλγορίθμους
    h. Αποτελέσματα ελέγχων
    i. Μελέτες
    j. Υποδείγματα
    k. Σχέδια / Τοπολογίες / Διαγράμματα
    l. Φωτογραφίες / Βίντεο / Ηχογραφήσεις
    m. Σκίτσα
    n. Προδιαγραφές ή άλλα επαγγελματικά μυστικά
    o. Τεχνογνωσία ή επιχειρηματικές ιδέες
3. Όταν η αποκάλυψη της απόρρητης πληροφορίας σε τρίτο πρόσωπο είναι αναγκαία, τότε πρέπει εκ των προτέρων να ζητηθεί έγγραφη εξουσιοδότηση από το άλλο μέρος.
4. Οποιαδήποτε αλλαγή γίνει σε αυτό το συμβόλαιο, πρέπει να σημειωθεί και να υπογραφεί με ημερομηνία και από τα δυο μέρη, διαφορετικά θα θεωρηθεί άκυρο.
5. Το παρόν συμφωνητικό εμπιστευτικότητας και τα σχετικά με αυτό θέματα, διέπονται από το Κυπριακό δίκαιο, ανεξαρτήτως παρεκκλίσεων από τις προβλεπόμενες διατάξεις και για κάθε διαφωνία ή διαφορά που προέρχεται από το παρόν συμφωνητικό, αποκλειστικά αρμόδια ορίζονται τα Κυπριακά δικαστήρια.
6. Το παρόν σύμφωνο έχει υπογραφεί από τον οργανισμό ΧΥΖ και τον συνεργάτη και έχουν λάβει από ένα γνήσιο αντίγραφο.

Όνομα: <όνομα>

Ιδιότητα: Ιδιοκτήτης Οργανισμού ΧΥΖ

Ημερομηνία: ……/……/……. [ηη/μμ/χχχχ]

Υπογραφή:……

Όνομα: <όνομα>

Ιδιότητα: Εργαζόμενος

Ημερομηνία: ……/……/……. [ηη/μμ/χχχχ]

Υπογραφή:……

Όνομα: <όνομα>

Ιδιότητα: Μάρτυρας

Ημερομηνία: ……/……/…… [ηη/μμ/χχχχ]

Υπογραφή:……

Συμβόλαιο 001 - Σύμβαση Εργασίας Αορίστου Χρόνου

Η παρούσα σύμβαση τίθεται σε ισχύ σήμερα ……/……/…… [ηη/μμ/χχχχ] από και μεταξύ των:

Οργανισμός ΧΥΖ, που εδρεύει στην οδό <διεύθυνση>, Κύπρος και Αριθμό μητρώου <αρ. μητρώου> και εκπροσωπείτε από τον/την κύριο/κυρία <όνομα>, ιδιοκτήτη

και

Ονοματεπώνυμο	
Αριθμός Ταυτότητας	
Χώρα έκδοσης της ταυτότητας	

που παρακάτω θα αναφέρεται ως «εργαζόμενος».

Τα δυο μέρη συναποδέχτηκαν τα εξής:

1. Ο τόπος εργασίας του εργαζόμενου θα είναι στα γραφεία του οργανισμού ΧΥΖ στην οδό <διεύθυνση>
2. Το αντικείμενο της εργασίας του εργαζόμενου θα είναι η: <αντικείμενο εργασίας>
3. Τα καθήκοντα του εργαζόμενου θα είναι:
    a. Xxx
    b. Yyy
    c. Zzz
4. Ο εργαζόμενος αποδέχεται να εργάζεται σε εγκαταστάσεις όπου παρακολουθούνται από κλειστό κύκλωμα παρακολούθησης (CCTV) και δίνει την συγκατάθεσή του για την καταγραφή των κινήσεων του περιμετρικά και εντός του οργανισμού.
5. Ο εργαζόμενος υποχρεούται να επιδεικνύει επιμέλεια στην εκτέλεση της εργασίας του, να συμμορφώνεται με τις οδηγίες των προϊστάμενων του καθώς και με τις πολιτικές του οργανισμού. Η μη συμμόρφωση με τις οδηγίες και τις πολιτικές του οργανισμού, θα έχει ως αποτέλεσμα την λήψη πειθαρχικής ενέργειας ή/και τον τερματισμό της απασχόλησης.
6. Απαγορεύεται στον εργαζόμενο να τηρεί προσωπικό αρχείο ή να μεταφέρει εκτός των εγκαταστάσεων δεδομένα του οργανισμού σε οποιαδήποτε μορφή (ψηφιακή ή έντυπη), εκτός αν έχει δοθεί προηγουμένως σχετική γραπτή άδεια. Οποιαδήποτε δεδομένα οποιασδήποτε μορφής προκύψουν από την εργασία του εργαζόμενου, αποτελούν περιουσιακά στοιχεία του οργανισμού.
7. Ο εργαζόμενος υποχρεούται να ενημερώσει γραπτώς για την αποχώρηση του από τον οργανισμό (τερματισμός εργασίας), 2 μήνες πριν.
8. Ο εργαζόμενος θα εργάζεται πέντε μέρες την εβδομάδα, 8 ώρες την ημέρα.
9. Η διάρκεια άδειας με αποδοχές που δικαιούται ο εργαζόμενος είναι <μέρες άδειας>
10. Η διάρκεια αναρρωτικής άδειας με αποδοχές που δικαιούται ο εργαζόμενος είναι <μέρες άδειας>. Η αναρρωτική άδεια πρέπει να δικαιολογείται με σχετική βεβαίωση του ιατρού.
11. Οι συνολικές μικτές μηνιαίες απολαβές του εργαζόμενου θα ανέρχονται σε <ποσό> ευρώ και θα καταβάλλονται ισόποσα την τελευταία μέρα κάθε ημερολογιακού μήνα.
12. Οποιαδήποτε αλλαγή γίνει στην παρούσα σύμβαση, πρέπει να σημειωθεί και να υπογραφεί με ημερομηνία και από τα δυο μέρη, διαφορετικά θα θεωρηθεί άκυρο.
13. Η παρούσα σύμβαση και τα σχετικά με αυτή θέματα, διέπονται από το Κυπριακό δίκαιο, ανεξαρτήτως παρεκκλίσεων από τις προβλεπόμενες διατάξεις και για κάθε διαφωνία ή διαφορά που προέρχεται από την παρούσα σύμβαση, αποκλειστικά αρμόδια ορίζονται τα Κυπριακά δικαστήρια.
14. Το παρόν συμβόλαιο έχει υπογραφεί από τον Οργανισμό ΧΥΖ και τον εργαζόμενο και έχουν λάβει από ένα γνήσιο αντίγραφο.

Όνομα: <όνομα>

Ιδιότητα: Ιδιοκτήτης Οργανισμού XYZ

Ημερομηνία: ……/……/…… [ηη/μμ/χχχχ]

Υπογραφή:……

Όνομα: <όνομα>

Ιδιότητα: Εργαζόμενος

Ημερομηνία: ……/……/…… [ηη/μμ/χχχχ]

Υπογραφή:……

Όνομα: <όνομα>

Ιδιότητα: Μάρτυρας

Ημερομηνία: ……/……/…… [ηη/μμ/χχχχ]

Υπογραφή:……

Συμβόλαιο 002 - Συμβόλαιο μεταξύ πρακτορείων (συμφωνία προθέσεων)

Το παρόν συμβόλαιο τίθεται σε ισχύ σήμερα ……/……/…… [ηη/μμ/χχχχ] από και μεταξύ των:

Οργανισμός XYZ, που εδρεύει στην οδό <διεύθυνση>, Κύπρος και Αριθμό μητρώου <αρ. μητρώου> και εκπροσωπείτε από τον/την κύριο/κυρία <όνομα>, ιδιοκτήτη

και

Όνομα Εταιρίας	
Έδρα Εταιρίας	
Εκπρόσωπος Εταιρίας	

που παρακάτω θα αναφέρεται ως «συνεργάτης».

Με το παρόν συμβόλαιο προθέσεων, ο συνεργάτης αναγνωρίζει και συμφωνεί ότι:

1. Είναι ενήμερος για την σχετική νομοθεσία και συγκεκριμένα τον «περί της σύμβασης κατά του εγκλήματος μέσω του διαδικτύου νόμο του 2004», της Κυπριακής Δημοκρατίας.
2. Θα υλοποιήσει και θα εφαρμόσει σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) σύμφωνα με τις απαιτήσεις της τελευταίας έκδοσης του διεθνούς προτύπου ISO 27001.
3. Θα καταθέσει σχετική αίτηση με τα στοιχεία των mobile agent, δικαιώματα πρόσβασης του στους πόρους και τις διαδρομές που θα ακολουθήσουν (Φόρμα 001).
4. Όλες οι ευαίσθητες πληροφορίες που θα μεταφέρονται από τους mobile agents πρέπει να είναι κρυπτογραφημένες.
5. Δεν θα προβεί σε καμία κακόβουλη ενέργεια εναντίον των mobile agents που θα εκτελούνται στα συστήματα του οργανισμού του. Σε άλλη περίπτωση ο οργανισμός XYZ θα προχωρήσει με καταγγελία στις αρμόδιες αρχές.
6. Δεν θα προβεί σε καμία κακόβουλη ενέργεια εναντίον της πλατφόρμας mobile agent του οργανισμού XYZ. Σε άλλη περίπτωση ο οργανισμός XYZ θα προχωρήσει με καταγγελία στις αρμόδιες αρχές.
7. Όλες οι εμπορικές πληροφορίες μεταξύ των δύο μερών πρέπει να μεταδίδονται κρυπτογραφημένες (πολιτική 010).
8. Θα γίνονται έλεγχοι/επιθεωρήσεις ανά 12 μήνες στο σύστημα διαχείρισης ασφάλειας πληροφοριών του οργανισμού του από επιθεωρητές του οργανισμού XYZ ή από ανεξάρτητο διαπιστευμένο φορέα πιστοποίησης.
9. Θα γίνονται έλεγχοι/επιθεωρήσεις ανά 6 μήνες στον πηγαίο κώδικα (source code) των mobile agents που θα εκτελούνται στα συστήματα του οργανισμού XYZ από προγραμματιστές του οργανισμού XYZ.
10. Πρέπει να γίνεται αυτόματος συγχρονισμός των ρολογιών όλων των hosts μέσω του time server (NTP) της Microsoft time.windows.com
11. Οποιαδήποτε αλλαγή γίνει σε αυτό το συμβόλαιο, πρέπει να σημειωθεί και να υπογραφεί με ημερομηνία και από τα δυο μέρη, διαφορετικά θα θεωρηθεί άκυρο.
12. Το παρόν συμβόλαιο και τα σχετικά με αυτό θέματα, διέπονται από το Κυπριακό δίκαιο, ανεξαρτήτως παρεκκλίσεων από τις προβλεπόμενες διατάξεις και για κάθε διαφωνία ή διαφορά που προέρχεται από το παρόν συμφωνητικό, αποκλειστικά αρμόδια ορίζονται τα Κυπριακά δικαστήρια.
13. Το παρόν συμβόλαιο έχει υπογραφεί από τον Οργανισμό XYZ και τον συνεργάτη και έχουν λάβει από ένα γνήσιο αντίγραφο.

Όνομα: <όνομα>

Ιδιότητα: Ιδιοκτήτης Οργανισμού XYZ

Ημερομηνία: ……/……/…… [ηη/μμ/χχχχ]

Υπογραφή:……

Όνομα: <όνομα>

Ιδιότητα: Μάρτυρας

Ημερομηνία: ……/……/…… [ηη/μμ/χχχχ]

Υπογραφή:……

Όνομα: <όνομα>

Ιδιότητα: Εργαζόμενος

Ημερομηνία: ……/……/…… [ηη/μμ/χχχχ]

Υπογραφή:……

Παράρτημα Η

Δήλωση Εφαρμοσιμότητας (Statement of Applicability)

Η.1 Δήλωση Εφαρμοσιμότητας (Statement of Applicability)

Statement of Applicability (Version 1.0)			
Έλεγχος ISO 27001:2013	**Εφαρμογή;**	**Αναφορά**	**Δικαιολογία**
A.05.01.01 Πολιτικές ασφάλειας πληροφοριών	Ναι	Διαδικασία 001	N/A
A.05.01.02 Ανασκόπηση πολιτικών ασφάλειας	Ναι	Διαδικασία 001	N/A
A.06.01.01 Ρόλοι και υπευθυνότητες σχετικές με την ασφάλεια πληροφοριών	Ναι	Παράγραφος 5.3 Οργανωτικοί ρόλοι, ευθύνες και εξουσίες	N/A
A.06.01.02 Διαχωρισμός Ρόλων και υπευθυνοτήτων	Ναι	Παράγραφος 5.3 Οργανωτικοί ρόλοι, ευθύνες και εξουσίες	N/A
A.06.01.03 Επικοινωνία με τις αρχές	Ναι	Πολιτική 001	N/A
A.06.01.04 Επικοινωνία με ομάδες ιδικών ενδιαφερόντων	Ναι	Πολιτική 001	N/A
A.06.01.05 Η ασφάλεια πληροφοριών στην διαχείριση έργων	Ναι	Πολιτική 002	N/A
A.06.02.01 Πολιτική κινητών συσκευών	Ναι	Πολιτική 003	N/A
A.06.02.02 Εργασία εξ αποστάσεως	Όχι	Πολιτική 003	Δεν επιτρέπεται η εξ αποστάσεως εργασία
A.07.01.01 Έλεγχος ιστορικού	Ναι	Πολιτική 004	N/A
A.07.01.02 Όροι και προϋποθέσεις εργοδότησης	Ναι	Πολιτική 004	N/A
A.07.02.01 Ευθύνες διοίκησης	Ναι	Πολιτική 004	N/A
A.07.02.02 Ευαισθητοποίηση και εκπαίδευση σε θέματα ασφάλειας πληροφοριών	Ναι	Πολιτική 004	N/A
A.07.02.03 Πειθαρχική διαδικασία	Ναι	Διαδικασία 002	N/A
A.07.03.01 Τερματισμός ή αλλαγή υπευθυνοτήτων	Ναι	Πολιτική 004	N/A
A.08.01.01 Καταγραφή περιουσιακών στοιχείων	Ναι	Παράγραφοι 6.1.2 και 6.1.3 Διαχείριση κινδύνων	N/A
A.08.01.02 Ιδιοκτησία περιουσιακών στοιχείων	Ναι	Παράγραφοι 6.1.2 και 6.1.3 Διαχείριση κινδύνων	N/A
A.08.01.03 Αποδεκτή χρήση περιουσιακών στοιχείων	Ναι	Πολιτική 006	N/A
A.08.01.04 Επιστροφή περιουσιακών στοιχείων	Ναι	Πολιτική 004	N/A
A.08.02.01 Διαβάθμιση περιουσιακών στοιχείων	Ναι	Πολιτική 005	N/A
A.08.02.02 Χαρακτηρισμός πληροφοριών	Ναι	Πολιτική 005	N/A
A.08.02.03 Χειρισμός των περιουσιακών στοιχείων	Ναι	Πολιτική 005	N/A
A.08.03.01 Διαχείριση αφαιρούμενων μέσων	Ναι	Διαδικασία 003	N/A
A.08.03.02 Καταστροφή μέσων αποθήκευσης	Ναι	Διαδικασία 003	N/A
A.08.03.03 Φυσική μεταφορά μέσων αποθήκευσης	Ναι	Διαδικασία 003	N/A
A.09.01.01 Πολιτική ελέγχου πρόσβασης	Ναι	Πολιτική 008	N/A
A.09.01.02 Πρόσβαση στα δίκτυα και υπηρεσίες δικτύου	Ναι	Πολιτική 008	N/A
A.09.02.01 Εγγραφή και διαγραφή χρηστών	Ναι	Διαδικασία 004	N/A
A.09.02.02 Παροχή πρόσβασης χρηστών	Ναι	Διαδικασία 004	N/A
A.09.02.03 Διαχείριση προνομιακών δικαιωμάτων πρόσβασης	Ναι	Πολιτική 008	N/A

Α.09.02.04 Διαχείριση στοιχείων αυθεντικοποίησης χρηστών	Ναι	Πολιτική 008	N/A
Α.09.02.05 Ανασκόπηση δικαιωμάτων πρόσβασης χρηστών	Ναι	Πολιτική 008	N/A
Α.09.02.06 Αφαίρεση η προσαρμογή δικαιωμάτων πρόσβασης χρηστών	Ναι	Διαδικασία 004	N/A
Α.09.03.01 Χρήση των στοιχείων αυθεντικοποίησης χρηστών	Ναι	Πολιτική 009	N/A
Α.09.04.01 Περιορισμός πρόσβασης σε πληροφορίες	Ναι	Πολιτική 008	N/A
Α.09.04.02 Διαδικασίες ασφαλούς πρόσβασης σε συστήματα και υπηρεσίες	Ναι	Διαδικασίες 004	N/A
Α.09.04.03 Σύστημα διαχείρισης κωδικών	Ναι	Πολιτική 009	
Α.09.04.04 Χρήση εργαλείων με προνομιακή πρόσβαση	Ναι	Διαδικασίες 004	N/A
Α.09.04.05 Έλεγχος πρόσβασης στον πηγαίο κώδικα	Ναι	Πολιτική 008	N/A
Α.10.01.01 Πολιτική χρήσης κρυπτογραφικών ελέγχων	Ναι	Πολιτική 010	N/A
Α.10.01.02 Διαχείριση κλειδιών	Ναι	Πολιτική 010	N/A
Α.11.01.01 Περιμετρική ασφάλεια	Ναι	Σχεδιασμός 002	N/A
Α.11.01.02 Έλεγχοι φυσικής πρόσβασης	Ναι	Σχεδιασμός 002	N/A
Α.11.01.03 Ασφάλεια γραφείων, δωματίων και άλλων εγκαταστάσεων	Ναι	Σχεδιασμός 002	N/A
Α.11.01.04 Προστασία από εξωτερικές και περιβαλλοντικές απειλές	Ναι	Σχεδιασμός 002	N/A
Α.11.01.05 Εργασία σε ασφαλείς περιοχές	Ναι	Σχεδιασμός 002	N/A
Α.11.01.06 Σημεία φόρτωσης και εκφόρτωσης	Όχι	N/A	Δεν υπάρχουν περιοχές φόρτωσης/εκφόρτωσης
Α.11.02.01 Τοποθέτηση και προστασία εξοπλισμού	Ναι	Σχεδιασμός 001	N/A
Α.11.02.02 Εργαλεία υποστήριξης	Ναι	Σχεδιασμός 001	N/A
Α.11.02.03 Ασφάλεια καλωδιώσεων	Ναι	Πολιτική 015	N/A
Α.11.02.04 Συντήρηση εξοπλισμού	Ναι	Σχεδιασμός 001	N/A
Α.11.02.05 Αφαίρεση περιουσιακών στοιχείων	Ναι	Συμβόλαιο 001	N/A
Α.11.02.06 Ασφάλεια εξοπλισμού και περιουσιακών στοιχείων εκτός των κτηριακών εγκαταστάσεων	Ναι	Πολιτική 013	N/A
Α.11.02.07 Ασφαλής καταστροφή ή επαναχρησιμοποίηση εξοπλισμού	Ναι	Διαδικασία 003	N/A
Α.11.02.08 Εξοπλισμός χωρίς επιτήρηση	Ναι	Πολιτική 011	N/A
Α.11.02.09 Πολιτική καθαρής οθόνης / καθαρού γραφείου	Ναι	Πολιτική 011	N/A
Α.12.01.01 Τεκμηριωμένες διαδικασίες λειτουργιών	Ναι	Διαδικασίες 001 - 012	
Α.12.01.02 Αλλαγές στο ΣΔΑΠ	Ναι	Διαδικασία 012	N/A
Α.12.01.03 Διαχείριση χωρητικοτήτων	Ναι	Πολιτική 013	N/A
Α.12.01.04 Διαχωρισμός περιβαλλόντων ανάπτυξης, ελέγχου και λειτουργίας	Ναι	Πολιτική 015	N/A
Α.12.02.01 Έλεγχοι κατά κακόβουλου λογισμικού	Ναι	Πολιτική 013	N/A

A.12.03.01 Αντίγραφα ασφάλειας πληροφοριών	Ναι	Πολιτική 013	N/A
A.12.04.01 Καταγραφή συμβάντων	Ναι	Πολιτική 012	N/A
A.12.04.02 Προστασία αρχείων καταγραφών συμβάντων	Ναι	Πολιτική 012	N/A
A.12.04.03 Αρχεία καταγραφής διαχειριστών	Ναι	Πολιτική 012	N/A
A.12.04.04 Συγχρονισμός ρολογιών	Ναι	Πολιτική 012	N/A
A.12.05.01 Εγκατάσταση λογισμικού σε συστήματα	Ναι	Πολιτική 013	N/A
A.12.06.01 Διαχείριση τεχνικών ευπαθειών	Ναι	Διαδικασία 006	N/A
A.12.06.02 Περιορισμοί στην εγκατάσταση εφαρμογών	Ναι	Πολιτική 013	N/A
A.12.07.01 Έλεγχοι επιθεώρησης συστημάτων πληροφορικής	Ναι	Πολιτική 014	N/A
A.13.01.01 Έλεγχοι δικτύου	Ναι	Πολιτική 015	N/A
A.13.01.02 Ασφάλεια υπηρεσιών δικτύου	Ναι	Πολιτική 015	N/A
A.13.01.03 Διαχωρισμός στα δίκτυα	Ναι	Πολιτική 015	N/A
A.13.02.01 Πολιτικές και διαδικασίες μεταφοράς πληροφοριών	Ναι	Πολιτική 010	N/A
A.13.02.02 Συμφωνίες μεταφοράς πληροφοριών	Ναι	Συμβόλαιο 002	N/A
A.13.02.03 Ηλεκτρονική αλληλογραφία	Ναι	Πολιτική 010	N/A
A.13.02.04 Σύμφωνα εμπιστευτικότητας	Ναι	Πολιτική 007	N/A
A.14.01.01 Ανάλυση και χαρακτηριστικά απαιτήσεων ασφάλειας των πληροφοριών	Ναι	Διαδικασία 006	N/A
A.14.01.02 Ασφάλεια υπηρεσιών σε δημόσια δίκτυα	Ναι	Πολιτική 010	N/A
A.14.01.03 Προστασία συναλλαγών πληροφοριών υπηρεσιών	Ναι	Πολιτική 010	N/A
A.14.02.01 Πολιτική ασφαλούς ανάπτυξης λογισμικού	Ναι	Πολιτική 016	N/A
A.14.02.02 Διαδικασίες αλλαγής συστημάτων ανάπτυξης λογισμικού	Ναι	Πολιτική 016	N/A
A.14.02.03 Τεχνική ανασκόπηση εφαρμογών μετά από αλλαγή πλατφόρμας	Ναι	Πολιτική 016	N/A
A.14.02.04 Περιορισμός αλλαγών σε πακέτα εφαρμογών	Ναι	Πολιτική 016	N/A
A.14.02.05 Αρχές ασφαλούς ανάπτυξης συστημάτων	Ναι	Πολιτική 016, Διαδικασία 008	N/A
A.14.02.06 Ασφαλές περιβάλλον ανάπτυξης εφαρμογών	Ναι	Πολιτική 016	N/A
A.14.02.07 Ανάπτυξη εφαρμογών από τρίτους	Όχι	N/A	Η ανάπτυξη του λογισμικού γίνεται εξολοκλήρου από τον Οργανισμό
A.14.02.08 Έλεγχος ασφάλειας συστημάτων	Ναι	Πολιτική 016	N/A
A.14.02.09 Αποδοχή ελέγχων συστημάτων	Ναι	Πολιτική 016	N/A
A.14.03.01 Ασφάλεια δεδομένων ελέγχων	Ναι	Πολιτική 016	N/A
A.15.01.01 Πολιτική ασφάλειας για την σχέση με τους προμηθευτές	Ναι	Πολιτική 017	N/A
A.15.01.02 Αντιμετώπιση των θεμάτων ασφάλειας στις συμφωνίες με τους προμηθευτές	Ναι	Πολιτική 017, Διαδικασία 007	N/A

A.15.01.03 Αλυσίδα προμήθειας πληροφοριακών και τηλεπικοινωνιακών τεχνολογιών	Ναι	Πολιτική 017, Διαδικασία 007	N/A
A.15.02.01 παρακολούθηση και ανασκόπηση των υπηρεσιών των προμηθευτών	Ναι	Πολιτική 017	N/A
A.15.02.02 Διαχείριση αλλαγών σε υπηρεσίες προμηθευτών	Ναι	Πολιτική 017	N/A
A.16.01.01 Ευθύνες και διαδικασίες στα περιστατικά ασφαλείας	Ναι	Διαδικασία 009	N/A
A.16.01.02 Αναφορά περιστατικών ασφαλείας	Ναι	Διαδικασία 009	N/A
A.16.01.03 Αναφορά αδυναμιών ασφάλειας	Ναι	Διαδικασία 009	N/A
A.16.01.04 Assessment of and decision on Information security events	Ναι	Διαδικασία 009	N/A
A.16.01.05 Αντίδραση στα περιστατικά ασφαλείας	Ναι	Διαδικασία 009	N/A
A.16.01.06 Μαθαίνοντας από τα περιστατικά ασφαλείας	Ναι	Διαδικασία 009	N/A
A.16.01.07 Συλλογή αποδεικτικών στοιχείων	Ναι	Διαδικασία 009	N/A
A.17.01.01 Σχεδιασμός επιχειρησιακής συνέχειας	Ναι	Σχεδιασμός 001	N/A
A.17.01.02 Υλοποίηση σχεδιασμού επιχειρησιακής συνέχειας	Ναι	Σχεδιασμός 001	N/A
A.17.01.03 Επαλήθευση, ανασκόπηση και αξιολόγηση του Υλοποίηση σχεδιασμού επιχειρησιακής συνέχειας	Ναι	Σχεδιασμός 001	N/A
A.17.02.01 Διαθεσιμότητα εγκαταστάσεων επεξεργασίας δεδομένων	Ναι	Σχεδιασμός 001	N/A
A.18.01.01 Αναγνώριση νομικών και συμφωνητικών απαιτήσεων του οργανισμού	Ναι	Πολιτική 007	N/A
A.18.01.02 Πνευματικά δικαιώματα	Ναι	Πολιτική 007	N/A
A.18.01.03 Προστασία αρχείων καταγραφών		Πολιτική 007	N/A
A.18.01.04 Ιδιωτικότητα και προστασία προσωπικών δεδομένων	Ναι	Εφαρμογή του Γενικού Κανονισμού της Ε.Ε για την Προστασία Δεδομένων (GDPR)	N/A
A.18.01.05 Ρύθμιση κρυπτογραφικών ελέγχων	Ναι	Πολιτική 007	N/A
A.18.02.01 Ανεξάρτητη ανασκόπηση του ΣΔΑΠ	Ναι	Ετήσιες επιθεωρήσεις από διαπιστευμένο φορέα πιστοποίησης. Τα αποτελέσματα της επιθεώρησης (report) στέλνονται στην διοίκηση.	N/A
A.18.02.02 Συμμόρφωση με πολιτικές ασφάλειας και πρότυπα	Ναι	Διαδικασία 010	N/A
A.18.02.03 Τεχνική ανασκόπηση συμμόρφωσης	Ναι	Πολιτική 014	N/A

Ιστορικό Αναθεώρησης

Ημερομηνία	**Υπεύθυνος**	**Περίληψη Αλλαγών**
29/11/2018	Διευθυντής Ασφάλειας Πληροφοριών	Πρώτη έκδοση

Εγκρίθηκε από

Υπογραφή: _____

Ημερομηνία: _____

Παράρτημα Θ
Πηγαίος Κώδικας

0.1 Host_A.java (Writer)

```java
// Host A
// Compile: javac Host_A.java
// Run: java Host_A <keystore password> <key password>

import javax.crypto.Cipher;
import java.io.InputStream;
import java.security.*;
import java.util.Base64;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;
import java.io.FileInputStream;
import java.io.FileWriter;

import static java.nio.charset.StandardCharsets.UTF_8;

import java.util.*;

public class Host_A {

    public static String keystore_password, key_password;

    public static KeyPair getKeyPairFromKeyStore() throws Exception {

        InputStream ins = Host_A.class.getResourceAsStream("/keystore_of_host_A.jceks")
;

        KeyStore keyStore = KeyStore.getInstance("JCEKS");
        keyStore.load(ins, keystore_password.toCharArray());   //Keystore password
        KeyStore.PasswordProtection keyPassword = new KeyStore.PasswordProtection(key_p
assword.toCharArray()); //Key password

        KeyStore.PrivateKeyEntry privateKeyEntry = (KeyStore.PrivateKeyEntry) keyStore.
getEntry("host_a", keyPassword);

        java.security.cert.Certificate cert = keyStore.getCertificate("host_b");
        PublicKey publicKey = cert.getPublicKey();
        PrivateKey privateKey = privateKeyEntry.getPrivateKey();

        return new KeyPair(publicKey, privateKey);
    }

    public static String sign(String plainText, PrivateKey privateKey) throws Exception
 {
        Signature privateSignature = Signature.getInstance("SHA256withRSA");
        privateSignature.initSign(privateKey);
        privateSignature.update(plainText.getBytes(UTF_8));

        byte[] signature = privateSignature.sign();

        return Base64.getEncoder().encodeToString(signature);
    }

    public static String encrypt(String plainText, PublicKey publicKey) throws Exceptio
n {
        Cipher encryptCipher = Cipher.getInstance("RSA");
        encryptCipher.init(Cipher.ENCRYPT_MODE, publicKey);

        byte[] cipherText = encryptCipher.doFinal(plainText.getBytes(UTF_8));

        return Base64.getEncoder().encodeToString(cipherText);
    }

    public static void main(String[] args) throws Exception {
        keystore_password = args[0];
```

```
60.         key_password = args[1];
61.
62.         KeyPair pair = getKeyPairFromKeyStore();
63.
64.         /*
65.         // Get Public key of B (manual)
66.         CertificateFactory fact = CertificateFactory.getInstance("X.509");
67.         FileInputStream is_of_b = new FileInputStream("host_b_pub.cer");
68.         X509Certificate cer_of_b = (X509Certificate) fact.generateCertificate(is_of_b);
69.         PublicKey publicKey_of_b = cer_of_b.getPublicKey();
70.         */
71.
72.         //Our secret message (must be 245 bytes (characters))
73.         Date date = new Date();
74.         String message = date.toString() + " - CONFIDENTIAL INFO: " + args[2];
75.
76.         //Let's sign our message
77.         String signature = sign(message, pair.getPrivate());
78.         //Encrypt the message for Host B
79.         String cipherText = encrypt(message, pair.getPublic());
80.
81.         System.out.println("\nSignature: "+signature+"\n");
82.         System.out.println("\nEncrypted Data: "+cipherText);
83.         try {
84.             // Save Signature
85.             FileWriter sig_data_file = new FileWriter("data_sig.txt");
86.             sig_data_file.write(signature);
87.             sig_data_file.close();
88.
89.             // Save Encrypted Message
90.             FileWriter enc_data_file = new FileWriter("enc_data.txt");
91.             enc_data_file.write(cipherText);
92.             enc_data_file.close();
93.         } catch (Exception ex) {
94.             System.out.println(ex);
95.         }
96.         Thread.sleep(3000);
97.     }
98. }
```

0.2 Host_B.java (Reader)

```java
// Host B
// Compile: javac Host_B.java
// Run: java Host_B <keystore password> <key password>

import javax.crypto.Cipher;
import java.io.InputStream;
import java.security.*;
import java.util.Base64;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;
import java.io.FileInputStream;
import java.io.*;
import java.nio.file.*;
import static java.nio.charset.StandardCharsets.UTF_8;
import java.util.*;

public class Host_B {

    public static String keystore_password, key_password;

    public static KeyPair getKeyPairFromKeyStore() throws Exception {

        InputStream ins = Host_B.class.getResourceAsStream("/keystore_of_host_B.jceks")
;

        KeyStore keyStore = KeyStore.getInstance("JCEKS");
        keyStore.load(ins, keystore_password.toCharArray());   //Keystore password
        KeyStore.PasswordProtection keyPassword = new KeyStore.PasswordProtection(key_p
assword.toCharArray()); //Key password

        KeyStore.PrivateKeyEntry privateKeyEntry = (KeyStore.PrivateKeyEntry) keyStore.
getEntry("host_b", keyPassword);

        java.security.cert.Certificate cert = keyStore.getCertificate("host_a");
        PublicKey publicKey = cert.getPublicKey();
        PrivateKey privateKey = privateKeyEntry.getPrivateKey();

        return new KeyPair(publicKey, privateKey);
    }

    public static String decrypt(String cipherText, PrivateKey privateKey) throws Excep
tion {
        byte[] bytes = Base64.getDecoder().decode(cipherText);

        Cipher decriptCipher = Cipher.getInstance("RSA");
        decriptCipher.init(Cipher.DECRYPT_MODE, privateKey);

        return new String(decriptCipher.doFinal(bytes), UTF_8);
    }

    public static boolean verify(String plainText, String signature, PublicKey publicKe
y) throws Exception {
        Signature publicSignature = Signature.getInstance("SHA256withRSA");
        publicSignature.initVerify(publicKey);
        publicSignature.update(plainText.getBytes(UTF_8));

        byte[] signatureBytes = Base64.getDecoder().decode(signature);

        return publicSignature.verify(signatureBytes);
    }

    public static String readFileAsString(String fileName) throws Exception {
       String data = "";
       data = new String(Files.readAllBytes(Paths.get(fileName)));
```

```
60.         return data;
61.     }
62.
63.      public static void main(String[] args) throws Exception {
64.
65.         keystore_password = args[0];
66.         key_password = args[1];
67.
68.         KeyPair pair = getKeyPairFromKeyStore();
69.
70.         /*
71.         // Get Public key of A (manual)
72.         CertificateFactory fact = CertificateFactory.getInstance("X.509");
73.         FileInputStream is_of_a = new FileInputStream ("host_a_pub.cer");
74.         X509Certificate cer_of_a = (X509Certificate) fact.generateCertificate(is_of_a);

75.         PublicKey publicKey_of_a = cer_of_a.getPublicKey();
76.         */
77.
78.         try {
79.         //Now decrypt it
80.         String decipheredMessage = decrypt(readFileAsString("enc_data.txt"), pair.getPr
    ivate());
81.         System.out.println("\n"+decipheredMessage+"\n");
82.
83.         //Let's check the signature
84.         boolean isCorrect = verify(decipheredMessage, readFileAsString("data_sig.txt"),
     pair.getPublic());
85.         System.out.println("Signature correct: " + isCorrect+"\n");
86.         // Write to log file
87.         Date date = new Date();
88.         FileWriter log_file = new FileWriter("Log.txt", true);
89.         log_file.write(date.toString() + "(Reader) | Signature correct: " + isCorrect +
     "\n");
90.         log_file.close();
91.         } catch (Exception ex) {
92.         System.out.println(ex);
93.         }
94.         Thread.sleep(3000);
95.     }
96. }
```

0.3 mytest.java (Mobile Agent)

```
1.  // Agent
2.  // Compile Command: javac -classpath aglets-2.5-gamma.jar mytest.java
3.
4.  package mytest;
5.
6.  import com.ibm.aglet.*;
7.  import com.ibm.aglet.event.*;
8.  import java.io.*;
9.  import java.nio.file.*;
10. import java.util.concurrent.TimeUnit;
11. import java.util.*;
12.
13. public class mytest extends Aglet {
14.
15.     boolean return_agent = false;
16.     BufferedReader br;
17.     String enc_data, data_sig, data_picked_timestamp;
18.     long start_time, end_time, timeelapsed;
19.
20.     class MyMobListener implements MobilityListener {
21.
22.         public void onDispatching(MobilityEvent ev) {
23.             if (return_agent == true) {
24.                 // Write to logfile
25.                 try{
26.                     Date date = new Date();
27.                     FileWriter log_file = new FileWriter("C:\\Host_B_Reader\\Log.txt",
    true);
28.                     log_file.write(date.toString() + "(Aglet) | Aglet " + getAgletID()
    + " dispatched\n");
29.                     log_file.close();
30.                 } catch (Exception ex) {
31.                     System.out.println(ex);
32.                 }
33.                 start_time = System.nanoTime();
34.             }
35.         }
36.
37.         public void onReverting(MobilityEvent ev) {
38.             //Code
39.         }
40.
41.         public void onArrival(MobilityEvent ev) {
42.             // When agent arrives to Host A
43.             System.out.println("My Test Arrived!\n");
44.             if (return_agent == true) {
45.                 try {
46.                     return_agent = false;
47.                     enc_data = readFileAsString("/home/george/Desktop/Host_A_Writer/enc
    _data.txt");
48.                     data_sig = readFileAsString("/home/george/Desktop/Host_A_Writer/dat
    a_sig.txt");
49.                     // Write to logfile
50.                     Date date = new Date();
51.                     data_picked_timestamp = date.toString() + "(Aglet) | Aglet " + getA
    gletID() + " picked the data\n";
52.                     System.out.println("Done! Bye Bye!\n\n");
53.                     //return back
54.                     dispatch(new java.net.URL(hostB));
55.                 } catch (Exception ex) {
56.
57.                     System.out.println(ex);
58.                 }
59.             } else {
```

```
60.                 // When agent returns back to Host B
61.                 end_time = System.nanoTime();
62.                 timeelapsed = (end_time-start_time)/ 1000000;
63.                 System.out.println("Time Elapsed: " + timeelapsed + "ms\n");
64.
65.                 return_agent = true;
66.                 System.out.println("Encrypted Data: " + enc_data + "\n");
67.                 System.out.println("Data Signature: " + data_sig);
68.
69.                 try {
70.                     // Save Signature
71.                     FileWriter sig_data_file = new FileWriter("C:\\Host_B_Reader\\data_
    sig.txt");
72.                     sig_data_file.write(data_sig);
73.                     sig_data_file.close();
74.
75.                     // Save Encrypted Message
76.                     FileWriter enc_data_file = new FileWriter("C:\\Host_B_Reader\\enc_d
    ata.txt");
77.                     enc_data_file.write(enc_data);
78.                     enc_data_file.close();
79.                 } catch (Exception ex) {
80.                     System.out.println(ex);
81.                 }
82.                 // Write to logfile
83.                 try {
84.                     Date date = new Date();
85.
86.                     FileWriter log_file = new FileWriter("C:\\Host_B_Reader\\Log.txt",
    true);
87.                     log_file.write(data_picked_timestamp);
88.                     log_file.write(date.toString() + "(Aglet) | Aglet " + getAgletID()
    + " arrived | Round Trip: " + timeelapsed + "ms\n");
89.                     log_file.close();
90.                 } catch (Exception ex) {
91.                     System.out.println(ex);
92.                 }
93.             }
94.         }
95.     }
96.
97.     public void onCreation(Object init) {
98.         System.out.println("My Test Created");
99.         MobilityListener mblistnr = new MyMobListener();
100.           addMobilityListener(mblistnr);
101.
102.           try {
103.               return_agent = true;
104.               //Go To Host A
105.               // Write to logfile
106.               try {
107.                   Date date = new Date();
108.                   FileWriter log_file = new FileWriter("C:\\Host_B_Reader\\Log.txt", t
    rue);
109.                   log_file.write(date.toString() + "(Aglet) | Aglet " + getAgletID() +
     " created\n");
110.                   log_file.close();
111.               } catch (Exception ex) {
112.                   System.out.println(ex);
113.               }
114.               dispatch(new java.net.URL(hostA));
115.           } catch (Exception ex) {
116.               System.out.println(ex);
117.           }
118.
119.       }
120.
121.       public static String readFileAsString(String fileName) throws Exception {
122.           String data = "";
```

```
            data = new String(Files.readAllBytes(Paths.get(fileName)));
            return data;
        }

        public void run() {
            //System.out.println("My Test Running...");
        }

        public void onDisposing() {
            System.out.println("My Test Quitting");
        }
    }
```

0.4 mytest2.java (Mobile Agent – DoS Attack)

```
// Agent
// Compile Command: javac -classpath aglets-2.5-gamma.jar mytest2.java

package mytest2;

import com.ibm.aglet.*;
import com.ibm.aglet.event.*;
import java.io.*;
import java.nio.file.*;
import java.util.concurrent.TimeUnit;
import java.util.*;

public class mytest2 extends Aglet {

    boolean return_agent = false;
    String hostA = "atp://192.168.111.129:4434";


    class MyCloneListener implements CloneListener{
        //before cloning
        public void onCloning(CloneEvent ev)  {}

        //after cloning
        public void onCloned(CloneEvent ev) {
            // DoS Attack (consume CPU & RAM)
            Vector v = new Vector();
            while (true){
                byte[] b = new byte[1000];
                v.add(b);
                Random rand = new Random();
                int radius = rand.nextInt(100);
                double calc = 3.14 * radius * radius;
                System.out.println("This is a DoS attack from -
=HoStB=- - Area: "+calc+ " - Aglet: " + getAgletID());
            }
        }

        //after cloning
        public void onClone(CloneEvent ev) {}
    }

    class MyMobListener implements MobilityListener {

        public void onDispatching(MobilityEvent ev) {}

        public void onReverting(MobilityEvent ev) {}

        public void onArrival(MobilityEvent ev) {
            return_agent = true;
        }
    }
```

```
51.
52.
53.     public void onCreation(Object init) {
54.         System.out.println("My Test Created");
55.         MobilityListener mblistnr = new MyMobListener();
56.         addMobilityListener(mblistnr);
57.         CloneListener clonelistnr = new MyCloneListener();
58.         addCloneListener(clonelistnr);
59.
60.         try {
61.             dispatch(new java.net.URL(hostA));
62.         } catch (Exception ex) {
63.             System.out.println(ex);
64.         }
65.     }
66.
67.     public void run() {
68.         //System.out.println("My Test Running...");
69.         if(return_agent == true){
70.             while(true){
71.                 try{
72.                     clone();
73.                 }catch (Exception e){
74.                     System.out.println(e);
75.                 }
76.             }
77.         }
78.     }
79.
80.     public void onDisposing() {
81.         System.out.println("My Test Quitting");
82.     }
83. }
```