Πολιτική Ασφαλείας

της Επιχείρησης

ΥΦΕΝ Α.Ε. - με τον διακριτικό τίτλο «HYPHEN SA», που εδρεύει στη Θεσσαλονίκη, στην οδό Λεωφόρος Βασ. Όλγας 24Β, ΤΚ 546 41, ΑΦΜ: 999972631, ΔΟΥ: ΦΑΕ Θεσσαλονίκης, Τηλ. 2310888125, Email: info@hyphensa.com

Φεβρουάριος 2019

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Περιεχόμενα

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Αρχείο Αλλαγών

Έκδοση	Ημερομηνία	Περιγραφή	Συγγραφέας
1.1	4/02/2019	Πρώτη έκδοση, Υποέκδοση 1	

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

1

1. Εισαγωγή

Η Πολιτική Ασφάλειας περιγράφει το σύνολο θεμελιωδών αρχών που καθορίζουν τον τρόπο με τον οποίο η Επιχείρηση προστατεύει την πληροφοριακή υποδομή που υποστηρίζει τις δραστηριότητες της Επιχείρησης, έτσι ώστε να επιτυγχάνει συγκεκριμένους στόχους ασφάλειας.

Σκοπός της Πολιτικής Ασφάλειας είναι να παράσχει στρατηγική καθοδήγηση στα στελέχη της Επιχείρησης για την προστασία των Πληροφοριακών Συστημάτων της (στο εξής ΠΣ). Η Πολιτική Ασφάλειας δεν πρέπει να είναι στατική, αλλά να προσαρμόζεται ακολουθώντας τις αλλαγές της πληροφοριακής υποδομής και του τεχνικοκοινωνικού περιβάλλοντος της Επιχείρησης.

Η προτεινόμενη Πολιτική Ασφάλειας βασίστηκε στις απαιτήσεις του Κανονισμού απαιτήσεις του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (GDPR), όπως αυτές εκφράζονται στις οδηγίες που περιλαμβάνει το ISO/ IEC 17799, καθώς και στις βασικές διαστάσεις των ορατών στρατηγικών κατευθύνσεων της Επιχείρησης, σε σχέση με την αξιοποίηση των Τεχνολογιών Πληροφορικής.

Η Πολιτική Ασφάλειας της Επιχείρησης καθοδηγεί τη λήψη αποφάσεων σε όλες τις βαθμίδες διοίκησης και αποτελεί αποτελεσματικό μέσο για την ασφάλεια των ΠΣ της Επιχείρησης. Η διασφάλιση της πληροφοριακής υποδομής, ως διαδικασία λήψης αποφάσεων, είναι ουσιαστικά εξαρτημένη από την ύπαρξη σχετικής πολιτικής ασφάλειας.

Η επιχείρηση καλείται να επιτύχει, με τη βοήθεια της Πολιτικής Ασφάλειας, τους ακόλουθους στόχους:

- Συμμόρφωση με τον Γενικό Κανονισμό ΕΕ/2016/679 "για την προστασία των φυσικών προσώπων έναντι επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)".

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

- Διασφάλιση της επιχειρησιακής της ικανότητας, στο βαθμό που εξαρτάται από την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα πληροφοριών και επικοινωνιών.
- Προστασία της επένδυσης που απαιτεί η λειτουργία των ΠΣ της Επιχείρησης.

Η Πολιτική Ασφάλειας των ΠΣ ανακλά την πρόθεση της Επιχείρησης να προστατέψει την πληροφοριακή της υποδομή. Η Πολιτική Ασφάλειας περιγράφει το σύνολο των αρχών και κανόνων που καθορίζουν τον τρόπο με τον οποίο η Επιχείρηση πρέπει να διαχειρίζεται και να προστατεύει τους πόρους της, έτσι ώστε να επιτυγχάνει συγκεκριμένους στόχους ασφάλειας.

Οι στόχοι αυτοί έχουν καθοριστεί από την ανάλυση επικινδυνότητας και συνοψίζονται στη σύννομη, αδιάλειπτη και αποτελεσματική λειτουργία των ΠΣ

Ο χαρακτήρας της Πολιτικής Ασφάλειας δεν αφορά μόνον τεχνικά ή μόνον οργανωτικά θέματα, αλλά αντιμετωπίζει με την ίδια προσοχή και τις δύο αυτές απόψεις διαχείρισης της ασφάλειας των ΠΣ.

1.1. Εμβέλεια της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας αφορά στα ΠΣ της Επιχείρησης που υποστηρίζουν δραστηριότητες της. Καλύπτει το σύνολο των πληροφοριών που διακινούνται, τυγχάνουν επεξεργασίας, ή αποθηκεύονται σε ηλεκτρονική μορφή, επεκτείνεται, όμως, και στις περιπτώσεις όπου οι ανωτέρω πληροφορίες μετατρέπονται σε άλλες μορφές (πχ. εκτυπώσεις).

1.2. Περιορισμοί

Η Πολιτική Ασφάλειας ΠΣ περιορίζεται στα συστήματα που υποστηρίζουν δραστηριότητες της Επιχείρησης, καθώς καταγραφή που πραγματοποιήθηκε αφορούσε αυτά τα συστήματα και οι νομικές και κανονιστικές υποχρεώσεις και το Αρχείο Δραστηριοτήτων του Άρθρου 30 του GDPR αφορά τις επεξεργασίες που διενεργεί η Επιχείρηση και τα τεχνικά μέσα που τις υποστηρίζουν.

Η διαμόρφωση της παρούσας πολιτικής έχει ως αφετηρία τα προβλεπόμενα στο πρότυπο ISO/IEC 17799 και η εφαρμογή της οδηγεί σε συμμόρφωση με το πρότυπο αυτό. Επίσης, καλύπτει τις σχετικές απαιτήσεις της Αρχής Προστασίας Προσωπικών Δεδομένων και της σχετικής νομοθεσίας.

Το Σχέδιο Κανονισμού για τη "διασφάλιση του απορρήτου κατά την παροχή τηλεπικοινωνιακών υπηρεσιών μέσω Δικτύων Κινητών Επικοινωνιών" της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών έχει ληφθεί υπόψη και έχει καθορίσει σε μεγάλο βαθμό τη δομή της Πολιτικής Ασφάλειας ΠΣ. Όμως, η παρούσα πολιτική δεν αναφέρεται στο φυσικό επικοινωνιακό δίκτυο και δεν καλύπτει τις προβλέψεις του Κανονισμού που το αφορούν, καθώς η μελέτη του φυσικού δικτύου δεν εντάσσεται στην οριοθέτηση της παρούσας μελέτης.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

1.3. Αξιοποίηση της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας βασίστηκε στις εκτιμήσεις των μελετητών του έργου σχετικά με τις απαιτήσεις ασφάλειας της οργάνωσης, λειτουργίας και τεχνικής υποδομής των ΠΣ της Επιχείρησης. Εντούτοις, η Πολιτική Ασφάλειας είναι άμεσα εξαρτημένη από τη φύση των δραστηριοτήτων της Επιχείρησης, τις κατευθύνσεις της Διοίκησης και το περιβάλλον λειτουργίας της Επιχείρησης.

Βασικά σημεία για την κατανόηση και αξιοποίηση της Πολιτικής Ασφάλειας αποτελούν οι εξής διαπιστώσεις:

- Η Πολιτική Ασφάλειας αποτελεί βασικό μέσο ανάπτυξης κουλτούρας ασφάλειας στα στελέχη και τους εργαζόμενους της Επιχείρησης. Αποτελεί γενικά διαθέσιμο κείμενο και πρέπει να ληφθεί μέριμνα, ώστε όλα τα μέλη του προσωπικού που έχουν ρόλο στη λειτουργία των ΠΣ, είτε ως χρήστες, είτε ως διαχειριστές, είτε ως διοικητικά στελέχη, να λάβουν γνώση της.
- Η Πολιτική Ασφάλειας δεν είναι απόλυτη ή στατική. Βασίστηκε στη καταγραφή της υφιστάμενης υποδομής καθώς και στο Αρχείο Δραστηριοτήτων του Άρθρου 30 του GDPR.
- Το παρόν κείμενο αποτελεί ένα ευέλικτο και αποτελεσματικό πρόπλασμα Πολιτικής Ασφάλειας. Η Επιχείρηση μπορεί να ορίσει, με βάση τις εκάστοτε προτεραιότητές της, το ακριβέστερο εύρος, ύφος και περιεχόμενο της Πολιτικής αυτής.

1.4. Βασικά στοιχεία της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας αποτελεί ένα πλαίσιο στο οποίο εντάσσεται ένα σύνολο εξειδικευμένων πολιτικών. Συγκεκριμένα η Πολιτική Ασφάλειας περιλαμβάνει τις εξής πολιτικές:

1) Πολιτική Διαχείρισης Ασφάλειας
2) Πολιτική Προσωπικού
3) Πολιτική Πρακτικών Θεμιτής Χρήσης
4) Πολιτική Προστασίας Προσωπικών Δεδομένων
5) Πολιτική Αναδόχων και Συνεργατών
6) Πολιτική Προστασίας ΠΣ
7) Πολιτική Ασφάλειας Ασύρματου Φορητού Η/Υ

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

2

2.Πολιτική Διαχείρισης Ασφάλειας

2.1. Εισαγωγή

Με την πολιτική Διαχείρισης Ασφάλειας η Επιχείρηση εκφράζει τη βούλησή της για τη διασφάλιση των ΠΣ που υποστηρίζουν τις δραστηριότητές της και παρέχει τις βασικές κατευθύνσεις για τη διαχείριση ασφάλειας των ΠΣ και τη συμμόρφωση της με τον Γενικό Κανονισμό ΕΕ/2016/679 "για την προστασία των φυσικών προσώπων έναντι επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)".

2.2. Σκοπός

Σκοπός της Πολιτικής Διαχείρισης Ασφάλειας είναι:

- Να εκφράσει ρητά τη βούληση της Επιχείρησης να διασφαλίσει τη λειτουργία των ΠΣ που υποστηρίζουν τις δραστηριότητες της.
- Να δώσει κατευθυντήριες οδηγίες στα στελέχη της Επιχείρησης για τον τρόπο με τον οποίο πρέπει να αντιμετωπίζουν τα ζητήματα ασφάλειας ΠΣ.
- Να προδιαγράψει ένα Σύστημα Διαχείρισης της Ασφάλειας των ΠΣ.

2.3. Εμβέλεια

Η Πολιτική απευθύνεται στα στελέχη της Επιχείρησης που ασκούν διοικητικά καθήκοντα που σχετίζονται με τις δραστηριότητες της, ή εποπτεύουν αυτές τις δραστηριότητες ή ασκούν διοίκηση σε τομείς που

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

υποστηρίζουν τη λειτουργία των ΠΣ. Απευθύνεται, επίσης, στο σύνολο του προσωπικού που υποστηρίζει τη λειτουργία των ΠΣ.

2.4. Γενικές Αρχές

Βούληση της διοίκησης

- Η Επιχείρηση αποδίδει υψηλή προτεραιότητα στην ασφάλεια των ΠΣ που υποστηρίζουν τις δραστηριότητες της.

Πολιτική ασφάλειας ΠΣ

- Η Επιχείρηση θεσπίζει και θέτει σε ισχύ την "Πολιτική Ασφάλειας ΠΣ". Η Πολιτική Ασφάλειας ΠΣ αποτελείται από την παρούσα Πολιτική Διαχείρισης Ασφάλειας ΠΣ, καθώς και από ένα σύνολο θεματικών Πολιτικών Ασφάλειας.

Υποστήριξη εφαρμογής της Πολιτικής Ασφάλειας ΠΣ

- Η Διοίκηση της Επιχείρησης υποστηρίζει την εφαρμογή της Πολιτικής Ασφάλειας ΠΣ εξασφαλίζοντας τους απαραίτητους για αυτό το σκοπό πόρους και μέσα.

Διοικητική και οργανωτική υποστήριξη διαχείρισης της ασφάλειας ΠΣ

- Με στόχο την αποτελεσματικότερη εφαρμογή της Πολιτικής Ασφάλειας ΠΣ, αναπτύσσεται η κατάλληλη διοικητική δομή, ορίζονται οι ρόλοι που είναι απαραίτητοι για τη διαχείρισης της ασφάλειας ΠΣ, καθορίζονται οι αρμοδιότητες για κάθε ρόλο και ανατίθενται οι ρόλοι στα κατάλληλα άτομα.

Συμμόρφωση με νομικό πλαίσιο

- Η Διοίκηση και τα στελέχη της Επιχείρησης προβαίνουν σε όλες τις ενέργειες που απαιτούνται για να γίνεται σεβαστή η νομοθεσία που αφορά την προστασία προσωπικών δεδομένων, το απόρρητο των επικοινωνιών, τα πνευματικά δικαιώματα, το ηλεκτρονικό έγκλημα και γενικά η νομοθεσία που αφορά τη χρήση ΠΣ.

2.5. Πολιτική Ασφάλειας ΠΣ

Βούληση της διοίκησης

- Η Πολιτική Ασφάλειας ΠΣ πρέπει να είναι έγγραφη και να έχει επικυρωθεί από τη Διοίκηση της Επιχείρησης.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

- Η Επιχείρηση προβαίνει σε όλες τις απαραίτητες ενέργειες, ώστε να ενημερώσει το προσωπικό για την Πολιτική Ασφάλειας ΠΣ και να εξασφαλίσει την άμεση και εύκολη πρόσβαση των υπαλλήλων στο πλήρες κείμενο της πολιτικής.
- Η Πολιτική Ασφάλειας ΠΣ αποτελείται από επί μέρους πολιτικές. Σε αυτές περιλαμβάνονται η Πολιτική Διαχείρισης Ασφάλειας ΠΣ, η Πολιτική Προσωπικού, η Πολιτική Θεμιτών Πρακτικών Χρήσης ΠΣ, η Πολιτική Προστασίας Προσωπικών Δεδομένων, η Πολιτική Αναδόχων και Συνεργατών και η Πολιτική Προστασίας ΠΣ.
- Η Πολιτική Ασφάλειας ΠΣ καθορίζεται με βάση την επικινδυνότητα που ενέχεται στη λειτουργία των ΠΣ, όπως αυτή αποτιμάται με την εκπόνηση μελέτης ανάλυσης επικινδυνότητας.
- Η Πολιτική Ασφάλειας ΠΣ πρέπει να τυγχάνει τακτικής ανασκόπησης και να αναθεωρείται και επικαιροποιείται σε περίπτωση μείζονων αλλαγών στα ΠΣ της Επιχείρησης, καθώς και σε περιπτώσεις σημαντικών μεταβολών του κοινωνικού και τεχνολογικού περιβάλλοντος, από τις οποίες προκύπτουν νέες απειλές, ευπάθειες, ή νέες ευκαιρίες βελτίωσης της ασφάλειας ΠΣ. Οι διαδικασίες αναθεώρησης της Πολιτικής περιλαμβάνονται στο Σχέδιο Ασφάλειας ΠΣ.
- Τα στελέχη της Επιχείρησης πρέπει να συμβουλεύονται την Πολιτική Ασφάλειας ΠΣ σε κάθε απόφασή τους, που αφορά ή μπορεί να επηρεάσει, άμεσα ή έμμεσα, την ασφάλεια των ΠΣ ή των δεδομένων.
- Η εφαρμογή της Πολιτικής Ασφάλειας ΠΣ είναι υποχρεωτική. Σε περίπτωση παραβίασης της Πολιτικής, η Επιχείρηση έχει το δικαίωμα να επιβάλλει κυρώσεις.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

3

3. Πολιτική Προσωπικού

3.1. Εισαγωγή

Ο σημαντικότερος παράγοντας στην ασφάλεια των ΠΣ είναι η συμπεριφορά και η δράση των ανθρώπων που μετέχουν της λειτουργίας των συστημάτων ως χρήστες ή ως διαχειριστές των συστημάτων ή ασκώντας διοικητικά καθήκοντα.

Η Επιχείρηση, αναγνωρίζοντας το σημαντικό ρόλο που διαδραματίζουν τα μέλη του προσωπικού στην προσπάθεια διασφάλισης της πληροφοριακής και επικοινωνιακής υποδομής της, ανέπτυξε και θέτει σε εφαρμογή την παρούσα Πολιτική Προσωπικού.

3.2. Σκοπός

Σκοπός της Πολιτικής Προσωπικού είναι:

- Η μείωση της επικινδυνότητας που συνδέεται με ανθρώπινα λάθη, με την πιθανή κατάχρηση των συστημάτων, καθώς και με κάθε εκούσια ή ακούσια ενέργεια που μπορεί να θέσει σε κίνδυνο τα ΠΣ.
- Η ενίσχυση της ενεργούς συμμετοχής του προσωπικού στη συλλογική προσπάθεια ενδυνάμωσης της ασφάλειας των ΠΣ.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

3.3. Εμβέλεια

Η Πολιτική Προσωπικού απευθύνεται στο σύνολο του προσωπικού της Επιχείρησης που κατά την άσκηση των καθηκόντων του επηρεάζει τη λειτουργία των ΠΣ της Επιχείρησης, είτε ως χρήστης, είτε ως διαχειριστής, είτε ασκώντας διοικητικά καθήκοντα.
Η Πολιτική Προσωπικού αφορά ιδιαίτερα τα στελέχη της Επιχείρησης που έχουν ως αρμοδιότητα τη διαχείριση του ανθρώπινου δυναμικού.
Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφαλείας.

3.4. Γενικές Αρχές

Ρόλος του ανθρώπινου δυναμικού

Η Επιχείρηση αποδίδει ιδιαίτερη βαρύτητα στο ρόλο που διαδραματίζει το ανθρώπινο δυναμικό στην προσπάθεια διασφάλισης των ΠΣ.

Ενίσχυση του ανθρώπινου δυναμικού

Η Επιχείρηση προβαίνει σε όλες τις απαιτούμενες ενέργειες για την ενίσχυση του προσωπικού της με μέσα, κατευθυντήριες οδηγίες, πληροφόρηση και γνώση, ώστε να συμβάλλει με τον πλέον αποτελεσματικό τρόπο στην ασφάλεια ΠΣ.

Υποχρέωση ενεργούς συμμετοχής

Όλα τα μέλη του προσωπικού έχουν την υποχρέωση να συμβάλλουν ενεργά στην ασφάλεια της πληροφορικής και επικοινωνιακής υποδομής της Επιχείρησης και να απέχουν από κάθε ενέργεια που μπορεί να θέσει σε κίνδυνο την ασφάλεια των ΠΣ και των Δεδομένων.

3.5. Οδηγίες και κανόνες ασφάλειας

<u>Α. Διαχείριση ανθρώπινου δυναμικού</u>

- Η Επιχείρηση επιλέγει προσωπικό με κατάλληλα τυπικά και ουσιαστικά προσόντα για να στελεχώσει θέσεις που είναι σημαντικές για την ασφαλή λειτουργία των ΠΣ.
- Η Επιχείρηση προβαίνει σε έλεγχο των τυπικών προσόντων και των συστάσεων του προσωπικού το οποίο προσλαμβάνεται για να αναλάβει αρμοδιότητες που είναι σημαντικές για την ασφαλή λειτουργία των ΠΣ.
- Η σύμβαση εργασίας του νέου προσωπικού περιλαμβάνει όρους που θα προβλέπουν τη συμμόρφωση με την Πολιτική Ασφάλειας ΠΣ.
- Το νέο προσωπικό υπογράφει δήλωση περί μη αποκάλυψης εταιρικών πληροφοριών, καθώς και πληροφοριών που αφορούν τους πελάτες, προμηθευτές και όποιον συνεργάζεται με την Επιχείρηση <θα πρέπει να το συνδέσουμε με ότι θα υπογράφει το προσωπικό>.
- Η Επιχείρηση σέβεται το δικαίωμα των υπαλλήλων της να προστατεύουν τα προσωπικά τους δεδομένα και δεν αποκαλύπτει σε άτομα που στερούνται ανάγκης γνώσης (need-to-know), εντός ή εκτός της Επιχείρησης, δεδομένα που αναφέρονται σε υπαλλήλους της.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

- Η Επιχείρηση, χωρίς να παραβιάζει τα έννομα δικαιώματα των υπαλλήλων της, διατηρεί το δικαίωμα πρόσβασης στα δεδομένα που δημιουργούνται και αποθηκεύονται στα ΠΣ της.

Β. Γενικές υποχρεώσεις προσωπικού

Όλα τα μέλη του προσωπικού έχουν την υποχρέωση να συμβάλλουν θετικά στην ασφάλεια των ΠΣ της Επιχείρησης.

- Όλα τα μέλη του προσωπικού οφείλουν να σέβονται την ιδιωτικότητα (privacy) των συναδέλφων τους.
- Το προσωπικό έχει την υποχρέωση να αποφεύγει τα δημόσια δυσφημιστικά σχόλια για πελάτες, συνεργάτες ή ανταγωνιστές της Επιχείρησης.
- Τα μέλη του προσωπικού έχουν την υποχρέωση να αποφεύγουν αρνητικά σχόλια για τους συναδέλφους τους ή για την ίδια την Επιχείρηση, παρά μόνο εάν αυτά εντάσσονται στις θεσμοθετημένες διαδικασίες διαλόγου, αξιολόγησης και ελέγχου της Επιχείρησης.
- Τα μέλη του προσωπικού έχουν την υποχρέωση να αναφέρουν οποιοδήποτε γεγονός ή ενέργεια θεωρούν ότι περιορίζει την ασφάλεια των ΠΣ. Η Διοίκηση οφείλει να χρησιμοποιεί αυτές τις πληροφορίες με διακριτικό τρόπο.

Γ. Πολιτική καθαρού γραφείου

Όλοι οι εργαζόμενοι θα πρέπει να ασφαλίζουν τα έγγραφά τους και τον προσωπικό χώρο εργασίας τους προτού φεύγουν από το γραφείο, το ντουλάπι, τον ηλεκτρονικό σταθμό εργασίας τους και το τηλέφωνο. Αυτό ισχύει ιδίως για τα γραφεία ανοιχτού σχεδίου, αλλά και σε άλλες περιπτώσεις, πρέπει να διασφαλιστεί ότι δεν επιτρέπεται η πρόσβαση σε έγγραφα, φορείς δεδομένων και εξαρτήματα πληροφορικής τα μη εξουσιοδοτημένα άτομα (επισκέπτες, προσωπικό καθαρισμού, μη εξουσιοδοτημένοι υπάλληλοι κτλ).

3.6. Αποχώρηση εργαζόμενου

Ενέργεια 1: Επιστροφή εξοπλισμού που έχει παρασχεθεί στον εργαζόμενο

Όλοι οι εργαζόμενοι θα πρέπει να επιστρέψουν όλα τα αγαθά της Επιχείρησης που έχουν στην κατοχή τους από την στιγμή που τερματίζεται η εργασία τους, το συμβόλαιο ή η συμφωνία τους. Η διαδικασία τερματισμού θα πρέπει να σχηματίζεται έτσι ώστε να περικλείει την επιστροφή του λογισμικού, εγγράφων, και του εξοπλισμού. Άλλα επιχειρηματικά αγαθά όπως κινητές υπολογιστικές συσκευές, πιστωτικές κάρτες, κάρτες πρόσβασης, λογισμικό, εγχειρίδια και αποθηκευμένη πληροφορία σε ηλεκτρονικά μέσα θα πρέπει επίσης να επιστραφούν.

Σε περιπτώσεις όπου ένας εργαζόμενος αγοράζει τον εξοπλισμό της Επιχείρησης ή χρησιμοποιεί τον δικό του προσωπικό εξοπλισμό, οι διαδικασίες θα πρέπει να ακολουθηθούν ώστε να διασφαλίσουν ότι όλη η σχετική πληροφορία μεταφέρεται στον οργανισμό και διαγράφεται ασφαλώς από τον εξοπλισμό του εργαζομένου. Σε περιπτώσεις όπου ένας εργαζόμενος έχει την γνώση που είναι σημαντική στις συνεχείς διαδικασίες ασφαλείας, αυτή η πληροφορία θα πρέπει να αρχειοθετείται και να μεταφέρεται στον οργανισμό.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Ενέργεια 2: Κατάργηση όλων των λογαριασμών και αφαίρεση των δικαιωμάτων πρόσβασης

Όλοι οι λογαριασμοί (πρόσβασης, ηλεκτρονικού ταχυδρομείου κ.τλ) θα πρέπει να καταργηθούν κατά τον τερματισμό εργασίας ενός εργαζόμενου.

Τα δικαιώματα πρόσβασης που θα πρέπει να αφαιρεθούν ή να προσαρμοστούν περιλαμβάνουν φυσική και λογική πρόσβαση, κλειδιά, κάρτες αναγνώρισης, εγκαταστάσεις επεξεργασίας πληροφοριών, και αφαίρεση από κάθε έγγραφο που τον αναγνωρίζει ως ενεργό μέλος τους οργανισμού.

Εάν ο αποχωρών εργαζόμενος γνωρίζει κωδικούς για λογαριασμούς που παραμένουν ενεργοί, αυτοί θα πρέπει να αλλαχτούν μετά τον τερματισμό ή την αλλαγή εργασίας, του συμβολαίου ή της συμφωνίας.

Τα δικαιώματα πρόσβασης για τα πληροφοριακά αγαθά και τις εγκαταστάσεις επεξεργασίας πληροφοριών θα πρέπει να μειωθούν ή να αφαιρεθούν πριν τερματιστεί η εργασία, βάσει της εκτίμησης των παραγόντων κινδύνου όπως:

- Εάν ο τερματισμός ή η αλλαγή γίνεται με πρωτοβουλία του εργοδότη (κίνδυνος διαφθοράς της πληροφορίας από τον εργαζόμενο).
- Τις τωρινές αρμοδιότητες του εργαζομένου.
- Την αξία των αγαθών στα οποία υπάρχει πρόσβαση.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

4

4. Πολιτική Πρακτικών Θεμιτής Χρήσης

4.1. Εισαγωγή

Η Πολιτική Θεμιτών Πρακτικών Χρήσης ΠΣ ρυθμίζει τα ζητήματα που αφορούν στη χρήση των ΠΣ που υποστηρίζουν τις δραστηριότητες της Επιχείρησης. Με την έκδοση της πολιτικής αυτής δίνεται η δυνατότητα στους χρήστες των ΠΣ να γνωρίζουν ποιες ενέργειές τους θεωρούνται επιτρεπτές και ποιες απαγορεύονται.

4.2. Σκοπός

Σκοπός της Πολιτικής Θεμιτών Πρακτικών Χρήσης ΠΣ είναι

- Να περιγράψει τον αποδεκτό τρόπο χρήσης του εξοπλισμού (υπολογιστικών και τηλεπικοινωνιακών συστημάτων) της Επιχείρησης. Αυτοί οι κανόνες υπάρχουν για να προστατεύσουν τον εργαζόμενο αλλά και την ίδια την Επιχείρηση. Ανάρμοστη χρήση θέτουν σε κίνδυνο την Επιχείρηση είτε μέσω της δημιουργίας αδυναμιών στην υποδομή οι οποίες θα ήταν δυνατό να γίνουν αντικείμενο επιθέσεων είτε μέσω ενεργειών οι οποίες παραβιάζουν τις νομικές υποχρεώσεις και την εκθέτουν.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

- Η αποτροπή πιθανών επιβλαβών συμβάντων που μπορεί να προκύψουν από κακή χρήση των ΠΣ της Επιχείρησης.
- Η προστασία των χρηστών των ΠΣ από τις συνέπειες που μπορεί να υποστούν από την εσφαλμένη χρήση των ΠΣ.
- Η διασφάλιση ότι οι χρήστες δεν θα καταχραστούν τις δυνατότητες χρήσης των ΠΣ που τους παρέχονται προκειμένου να προβούν σε παράνομες ενέργειες.

4.3. Εμβέλεια

Αυτή η πολιτική εφαρμόζεται σε κάθε χρήστη του δικτύου δεδομένων της Επιχείρησης

- επισκέπτες,
- μόνιμο προσωπικό,
- συμβασιούχοι,
- εξωτερικοί συνεργάτες,
- σύμβουλοι,
- προσωπικό που σχετίζονται με τρίτους.

Όσον αφορά τον εξοπλισμό, η πολιτική εφαρμόζεται σε όλο τον εξοπλισμό που κατέχει ή έχει ενοικιάσει η Επιχείρηση. Η Επιχείρηση στα πλαίσια της καλής λειτουργίας του δικτύου δεδομένων υποχρεούται να δίνει πρόσβαση στο δίκτυο στους χρήστες κατόπιν αποδοχής της πολιτικής αποδεκτής χρήσης και να λαμβάνει μέτρα στο μέτρο του δυνατού για την ασφάλεια των συστημάτων που διαχειρίζεται και μέτρα για την διασφάλιση του απόρρητου των τηλεπικοινωνιών μέσα στα όρια του δικτύου του. Επίσης, υποχρεούται να τηρεί τις αρχές προστασίας δεδομένων προσωπικού χαρακτήρα σύμφωνα με την ισχύουσα νομοθεσία και τις διαδικασίες που προβλέπονται από την πολιτική ασφάλειας του δικτύου.

4.4. Ομάδα Έργου

Η πολιτική αυτή απευθύνεται στα μέλη του προσωπικού της Επιχείρησης και σε όσους συνεργάτες της χρησιμοποιούν ΠΣ που υποστηρίζουν δραστηριότητες της.

Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας ΠΣ.

4.5. Γενικές Αρχές

Αξία των ΠΣ

- Τα ΠΣ συγκαταλέγονται στους πολυτιμότερους πόρους της Επιχείρησης και κάθε μέλος του προσωπικού έχει την υποχρέωση να τα χρησιμοποιεί με προσοχή.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Τα ΠΣ αποτελούν περιουσιακό στοιχείο

- Τα ΠΣ που προσφέρονται στο προσωπικό της Επιχείρησης αποτελούν περιουσιακό της στοιχείο και η χρήση τους πρέπει να γίνεται αποκλειστικά για τους σκοπούς της Επιχείρησης.

Υποχρεώσεις συνδεόμενες με τη χρήση των ΠΣ

- Η χρήση των ΠΣ συνεπάγεται την ανάληψη ευθυνών και υποχρεώσεων που περιγράφονται στην Πολιτική Θεμιτών Πρακτικών Χρήσης ΠΣ.

4.6. Οδηγίες και Κανόνες Ασφαλείας

4.6.1. Δικαιώματα και υποχρεώσεις χρηστών

- Το προσωπικό δικαιούται να χρησιμοποιεί τα ΠΣ της Επιχείρησης σύμφωνα με τα όσα προβλέπονται στην παρούσα Πολιτική Θεμιτών Πρακτικών Χρήσης ΠΣ.
- Το προσωπικό πρέπει να χρησιμοποιεί σωστά τα ΠΣ και να μην αρκείται στην κατά γράμμα εφαρμογή της Πολιτικής Θεμιτών Πρακτικών Χρήσης ΠΣ. Σε περίπτωση που κάποιο μέλος του προσωπικού αμφιβάλλει αν κάποια ενέργειά του είναι συμβατή με την πολιτική, θα πρέπει να απευθύνεται στον Υπεύθυνο Ασφάλειας/Διευθύνοντα Σύμβουλο της Επιχείρησης.
- Οι χρήστες έχουν το δικαίωμα να ενημερώνονται σχετικά με τα δεδομένα που συλλέγονται από την Επιχείρηση και αφορούν τη χρήση των ΠΣ από αυτούς.
- Τα δεδομένα που δημιουργούνται με τη χρήση των ΠΣ της Επιχείρησης αποτελούν ιδιοκτησία της Επιχείρησης.
- Οι χρήστες οφείλουν να σέβονται τους ελέγχους πρόσβασης (access controls), ακόμα και αν αυτοί είναι ανεπαρκείς.
- Οι χρήστες πρέπει να μην παραβιάζουν τους μηχανισμούς ασφάλειας, έστω και αν έχουν στόχο να καταδείξουν τα αδύναμα σημεία τους. Εάν θεωρούν ότι οι μηχανισμοί είναι ανεπαρκείς, οφείλουν να το υποδείξουν στον Υπεύθυνο Ασφάλειας ΠΣ. Ο Υπεύθυνος Ασφάλειας ΠΣ θα εξετάσει την υπόθεση, χωρίς να απαιτήσει αποδείξεις.
- Όσα μέλη του προσωπικού διαθέτουν φορητό υπολογιστή και τον χρησιμοποιούν για εργασιακούς σκοπούς πρέπει να συμμορφώνονται με τις πολιτικές που ισχύουν για το συμβατικό εξοπλισμό (προσωπικοί υπολογιστές κλπ.).
- Οι χρήστες υποχρεούνται να συμμορφώνονται με την νομοθεσία για την προστασία της πνευματικής ιδιοκτησίας.
- Απαγορεύεται η χρήση λογισμικού που δεν έχει αποκτηθεί με νόμιμο τρόπο.
- Απαγορεύεται η χρήση οποιουδήποτε υλικού ή λογισμικού που δεν είναι σε γνώση της Διεύθυνσης της Επιχείρησης.
- Απαγορεύεται οποιαδήποτε ενέργεια μη εξουσιοδοτημένης χαρτογράφησης του δικτύου της Επιχείρησης.
- Απαγορεύεται η χρήση μηχανισμού ασφάλειας (πχ. προσωπικά αναχώματα ασφάλειας (firewall), συστήματα προστασίας από ιομορφικό λογισμικό) που δεν έχουν την έγκριση του Υπεύθυνου Ασφάλειας ή της Διοίκησης της Επιχείρησης.
- Απαγορεύεται η χρήση μη εταιρικών συστημάτων για εταιρικές εργασίες.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

- Οι χρήστες οφείλουν να λαμβάνουν όλα τα μέτρα που υποδεικνύουν οι υπεύθυνοι της Επιχείρησης για τη διασφάλιση του απορρήτου των επικοινωνιών τους.
- Οι εργαζόμενοι στην Επιχείρηση απαγορεύεται να αποκαλύπτουν πληροφορίες που συνδέονται με (α) το περιεχόμενο ή την ουσία των επικοινωνιών των πελατών της Επιχείρησης, (β) στοιχεία σχετικά με υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα πρόσωπο ή (γ) άλλα προσωπικά δεδομένα των χρηστών των τηλεπικοινωνιακών υπηρεσιών, όπως αριθμούς τηλεφώνου ή διευθύνσεις.

4.6.2. Παρακολούθηση και έλεγχος εφαρμογής της πολιτικής

- Τα δεδομένα που δημιουργούνται με τη χρήση των ΠΣ της Επιχείρησης αποτελούν ιδιοκτησία της Επιχείρησης.
- Η χρήση των ΠΣ μπορεί να καταγράφεται και να παρακολουθείται από εξουσιοδοτημένα άτομα. Οι χρήστες ενημερώνονται εφάπαξ ότι οι ενέργειές τους καταγράφονται.
- Η Επιχείρηση διατηρεί το δικαίωμα να διενεργεί προγραμματισμένους ή έκτακτους ελέγχους για την τήρηση της Πολιτικής Θεμιτών Πρακτικών Χρήσης ΠΣ και για την τήρηση των πολιτικών που συμπεριλαμβάνονται στην Πολιτική Ασφάλειας ΠΣ. Τους ελέγχους πραγματοποιούν εξουσιοδοτημένα για το σκοπό αυτό άτομα (Ελεγκτές ΠΣ) και τα μέλη του προσωπικού οφείλουν να συνεργαστούν με αυτούς. Το προσωπικό έχει δικαίωμα να ενημερωθεί για τα μέσα ελέγχου, τα κριτήρια ελέγχου και τα αποτελέσματα των ελέγχων που το αφορούν.

4.6.3. Χρήση Προσωπικού Ηλεκτρονικού Υπολογιστή

Για να εξασφαλιστεί η εύρυθμη λειτουργία του Η/Υ και να διασφαλιστούν οι πληροφορίες που τηρούνται σε αυτόν, ο κάθε εργαζόμενος πρέπει:

- Να χρησιμοποιεί μόνο τους δικούς του κωδικούς πρόσβασης για να συνδεθεί, είτε με τον Η/Υ είτε με κάποιο πληροφοριακό σύστημα.
- Να αποσυνδέεται (log off) από τον Η/Υ του ή από το πληροφοριακό σύστημα, όταν δεν χρησιμοποιείται.
- Να ενημερώνει/επικαιροποιεί το λειτουργικό σύστημα του Η/Υ του με τις εκάστοτε εκδόσεις που δημοσιοποιούν οι κατασκευάστριες εταιρείες. Οι ενημερώσεις αυτές κατά ένα πολύ μεγάλο ποσοστό καλύπτουν κενά ασφάλειας. Σχετικό είναι το ΠΑΡΑΡΤΗΜΑ ΙΙ.
- Να βεβαιώνεται ότι το πρόγραμμα ανίχνευσης ιών (Antivirus), που είναι εγκατεστημένο στον Η/Υ του, λειτουργεί κανονικά και ενημερώνεται με τις νέες εκδόσεις καθημερινά.
- Οι έλεγχοι για ιούς που ξεκινούν, είτε από τον ίδιο το χρήστη είτε αυτόματα από τον Η/Υ, πρέπει να αφήνονται να ολοκληρωθούν και να μην τερματίζονται από το χρήστη.
- Όταν ένας σκληρός δίσκος ή οποιοσδήποτε άλλος αποθηκευτικός εξοπλισμός είναι εκτός λειτουργίας θα πρέπει να παραδίνεται στη Διεύθυνση της Επιχείρησης για καταστροφή, για να αποφευχθεί ο κίνδυνος ανάκτησης των πληροφοριών που τηρούνται σε αυτόν.
- Η εγκατάσταση των λογισμικών γίνεται μόνο από άτομα της Διεύθυνσης Πληροφορικής από άτομα/εταιρείες εξουσιοδοτημένες από τη Διοίκηση.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

4.6.4.Ασφαλής Χρήση του Διαδικτύου και του Ηλεκτρονικού Ταχυδρομείου

- Απαγορεύεται η χρήση του ηλεκτρονικού ταχυδρομείου για την αποστολή αυτόκλητων μηνυμάτων (unsolicited mail - spam).
- Οι υπηρεσίες ηλεκτρονικού ταχυδρομείου παρέχονται στο προσωπικό της Επιχείρησης για να χρησιμοποιούνται αποκλειστικά για τους σκοπούς της. Η Επιχείρηση δεν είναι υποχρεωμένη να προστατεύει τα ηλεκτρονικά μηνύματα ως προσωπικά δεδομένα των υπαλλήλων.
- Όλα τα ηλεκτρονικά μηνύματα συνοδεύονται από κείμενο που δηλώνει ότι όσα αναφέρονται σε αυτό δεν απηχούν κατ' ανάγκην τις απόψεις της Επιχείρησης.
- Οι χρήστες πρέπει να γνωρίζουν ότι η εμπιστευτικότητα των ηλεκτρονικών μηνυμάτων δεν μπορεί να διασφαλιστεί παρά μόνο εάν εφαρμόζονται ειδικές τεχνικές κρυπτογράφησης.
- Οι χρήστες πρέπει να γνωρίζουν ότι ο παραλήπτης ενός μηνύματος μπορεί να το διατηρήσει για απροσδιόριστο χρόνο, να το προωθήσει σε τρίτους ή ακόμα να αλλοιώσει το περιεχόμενό του και έπειτα να το προωθήσει σε τρίτους.
- Οι χρήστες πρέπει να γνωρίζουν ότι η πραγματική ταυτότητα του αποστολέα ενός μηνύματος μπορεί να είναι διαφορετική από την αναγραφόμενη στο μήνυμα.
- Η αποστολή μαζικών ηλεκτρονικών μηνυμάτων (bulk emails) σε ομάδες ατόμων, όπου τα στοιχεία τους είναι ορατά από όλους τους παραλήπτες, θεωρείται αποκάλυψη προσωπικών δεδομένων σε τρίτους, και συνεπώς παραβίαση της σχετικής νομοθεσίας. Για να αποφευχθεί η αποκάλυψη των στοιχείων των παραληπτών πρέπει τα στοιχεία (ονόματα/ηλεκτρονικές διευθύνσεις) να καταχωρούνται στα πεδία "Ιδιαίτερη Κοινοποίηση" (BCC: Blind Carbon Copy). Αν το πεδίο "Ιδιαίτερη Κοινοποίηση" δεν είναι ορατό κατά τη δημιουργία νέου ηλεκτρονικού μηνύματος, τότε ο χρήστης πρέπει να επιλέξει από το μενού "Προβολή του μηνύματος" (View Menu) την εντολή εμφάνισης "Ιδιαίτερη Κοινοποίηση" (Show BCC).
- Σε περίπτωση χρήσης κοινού τερματικού ή Η/Υ που δεν ανήκει στο χρήστη, ο χρήστης, αφού ολοκληρώσει την εργασία του, θα πρέπει να διαγράψει το ιστορικό πλοήγησης, την προσωρινή μνήμη (Cache memory) του φυλλομετρητή (browser) και τα μπισκοτάκια δεδομένων (Cookies).
- Η αποστολή μαζικών ηλεκτρονικών μηνυμάτων (bulk emails) θα γίνεται μόνο σε παραλήπτες που η Επιχείρηση έχει λάβει τη ρητή συναίνεσή τους και πάντα για τον σκοπό που έχει δώσει το υποκείμενο των δεδομένων τη συναίνεσή του.
- Ο χρήστης πρέπει να βεβαιώνεται ότι το ηλεκτρονικό μήνυμα που θα στείλει απευθύνεται στο σωστό παραλήπτη με τη σωστή ηλεκτρονική διεύθυνση.
- Οι χρήστες δεν πρέπει να χρησιμοποιούν τους λογαριασμούς ηλεκτρονικού ταχυδρομείου συναδέλφων τους. Όποτε απαιτείται περισσότερα του ενός πρόσωπα να χρησιμοποιούν ένα λογαριασμό, τότε δημιουργείται ειδικός λογαριασμός με όνομα που δε συνδέεται με κάποιο πρόσωπο (πχ. info@hyphensa.com, accounts@hyphensa.com, κλπ.).
- Δεν πρέπει να αποστέλλονται εμπιστευτικές πληροφορίες εκτός της Επιχείρησης με το ηλεκτρονικό ταχυδρομείο.
- Σε περίπτωση λήψης ηλεκτρονικού μηνύματος, το οποίο στάληκε εκ παραδρομής και δεν απευθύνεται στο συγκεκριμένο παραλήπτη, ο παραλήπτης πρέπει να προωθήσει το μήνυμα στο σωστό άτομο (όπου είναι δυνατό) και να ενημερώσει τον αποστολέα ανάλογα ζητώντας του να διαγράψει οριστικά το μήνυμα, διατηρώντας παράλληλα και την εμπιστευτικότητα του μηνύματος.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

- Η πρόσβαση στο Διαδίκτυο παρέχεται στο προσωπικό της Επιχείρησης για να χρησιμοποιηθεί για τους σκοπούς της Επιχείρησης και για τη βελτίωση των γνώσεων και δεξιοτήτων του ανθρώπινου δυναμικού της.
- Η Επιχείρηση διατηρεί το δικαίωμα να περιορίσει την πρόσβαση σε συγκεκριμένους ιστοτόπους (Web Sites) του Παγκόσμιου Ιστού (World Wide Web). Οι χρήστες που χρειάζονται πρόσβαση σε Ιστοτόπους που δεν έχουν εγκριθεί από την Επιχείρηση έχουν το δικαίωμα να υποβάλλουν σχετικό αίτημα στον Υπεύθυνο Ασφάλειας ΠΣ/Διεύθυνση της Επιχείρησης.
- Οι χρήστες πρέπει να γνωρίζουν ότι οι δυνατότητες των γραμμών που συνδέουν την Επιχείρηση με το Διαδίκτυο είναι πεπερασμένες και κατά συνέπεια η κατάχρηση των υπηρεσιών του Διαδικτύου (πχ. η λήψη μεγάλων αρχείων) περιορίζει τη χρήση του Διαδικτύου από τους συναδέλφους τους.
- Οι χρήστες πρέπει να αποφεύγουν την επίσκεψη σε Ιστοσελίδες (Web Pages) με παράνομο λογισμικό, μη πρέπον υλικό ή άλλο πειρατικό οπτικοακουστικό υλικό. Οι χρήστες πρέπει να γνωρίζουν ότι η επίσκεψη αυτών των Ιστοσελίδων μπορεί να θέσει σε κίνδυνο την ασφάλεια των ΠΣ.
- Σε περίπτωση αποχώρησης κάποιου υπαλλήλου από την Επιχείρηση, ο Υπεύθυνος Ασφαλείας πρέπει να ειδοποιεί για να διαγράψει το ηλεκτρονικό του ταχυδρομείο. Ο υπάλληλος, προτού αποχωρήσει, έχει την ευθύνη να μεταφέρει στον προϊστάμενό του τα ηλεκτρονικά μηνύματα, τα οποία κρίνονται αναγκαία.
- Απαγορεύεται:
    - Η εγκατάσταση λογισμικού μέσω διαδικτύου.
    - Το άνοιγμα μηνυμάτων, αρχείων ή επισυναπτόμενων από άγνωστο αποστολέα. Πολλά από αυτά περιέχουν μολυσμένα αρχεία από ιούς ή διαφημίζουν ακατάλληλο και παράνομο περιεχόμενο ή αποσκοπούν στην εξαπάτηση των χρηστών και την απόκτηση προσωπικών πληροφοριών.
    - Προσοχή στα μηνύματα με επισυναπτόμενα: είναι σημαντικό να αποφεύγει κανείς το άνοιγμα αρχείων ή εγγράφων που παραλαμβάνει από άγνωστο αποστολέα, είτε μέσω ηλεκτρονικής αλληλογραφίας είτε μέσω άλλων μέσων, γιατί μπορεί να περιέχουν ιό. Ακόμα και σε περιπτώσεις όπου ο αποστολέας είναι γνωστός, όμως το περιεχόμενο του μηνύματος ή το επισυναπτόμενο αρχείο είναι άσχετο ή περίεργο (π.χ. Ζητούνται προσωπικά δεδομένα), ο χρήστης θα πρέπει να επιβεβαιώσει μαζί του ότι αυτός έχει στείλει το αρχείο και ότι η χρήση του είναι ασφαλής. Ιδιαίτερη προσοχή πρέπει να δίνεται επίσης σε μηνύματα που προτρέπουν το χρήστη να ανοίξει το επισυναπτόμενο αρχείο και ισχυρίζονται πως προέρχονται από την ομάδα υποστήριξης κάποιου φορέα, τράπεζας, κλπ. Τέτοιου είδους μηνύματα θα πρέπει να αγνοούνται και να διαγράφονται.
    - Η αποστολή μηνυμάτων τύπου αλυσίδας (Chain mail) ή ανεπιθύμητων μηνυμάτων διαφημιστικού περιεχομένου ή προωθητικού περιεχομένου σε χρήστες που δεν έχουν αποδεχτεί εγγράφως τη λήψη τέτοιου είδους μηνύματος (Spam mail).

4.6.5. Δικαιώματα και Κωδικοί Πρόσβασης

Ο κωδικός πρόσβασης (Password) είναι το στοιχείο με το οποίο επαληθεύεται ότι, ο χρήστης που προσπαθεί να συνδεθεί είναι πραγματικά ο κάτοχος του ονόματος χρήστη (username). Οι ακόλουθες

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

οδηγίες μπορούν να προφυλάξουν το χρήστη από το να μάθει κάποιος τον κωδικό του και να έχει έτσι παράνομη πρόσβαση στον Η/Υ του ή σε κάποιο πληροφοριακό σύστημα ή και στο ηλεκτρονικό του ταχυδρομείο.

- Το όνομα χρήστη και ο κωδικός πρόσβασης πρέπει να είναι γνωστά μόνο στο χρήστη και να μην κοινοποιούνται σε τρίτους, έστω και εάν αυτοί είναι στενά συγγενικά πρόσωπα, υπάλληλοι της Επιχείρησης, ανώτερα διοικητικά στελέχη ή ακόμα και οι διαχειριστές των ΠΣ της Επιχείρησης.
- Απαγορεύεται η αποκάλυψη της μεθόδου με την οποία ο χρήστης έχει επιλέξει το συνθηματικό του.
- Απαγορεύεται στους χρήστες να γνωστοποιούν το συνθηματικό τους σε συναδέλφους τους, όταν πρόκειται να απουσιάσουν (πχ. λόγω αδείας ή ασθενείας). Οι χρήστες πρέπει να συμβουλεύονται τον Υπεύθυνο Ασφάλειας ΠΣ για τον τρόπο με τον οποίο μπορεί να επιτευχθεί η συνέχεια των εργασιών που έχουν αναλάβει.
- Οι χρήστες πρέπει να αλλάζουν το συνθηματικό τους σε κάθε περίπτωση που θεωρούν ότι μπορεί ή έχει ήδη αποκαλυφθεί.
- Τα συνθηματικά των χρηστών πρέπει να αλλάζουν τουλάχιστον κάθε τρεις μήνες.
- Ο κωδικός πρόσβασης δεν πρέπει δεν πρέπει να καταγράφεται πχ. να αναγράφεται σε χαρτί ή στο κινητό τηλέφωνο ή σε μηνύματα ηλεκτρονικού ταχυδρομείου, επιστολές κλπ.
- Απαγορεύεται η χρήση λειτουργιών αυτόματης συμπλήρωσης συνθηματικού, όπως η λειτουργία "remember password", καθώς και η αποθήκευση των συνθηματικών σε υπολογιστές ή συσκευές (tablets, κινητά τηλέφωνα κλπ.) χωρίς κρυπτογράφηση.
- κωδικός πρόσβασης πρέπει να είναι «ισχυρός» και πολύπλοκος. Δεν πρέπει να χρησιμοποιείται «αδύναμος» κωδικός, ο οποίος μπορεί εύκολα να προβλεφθεί. Μερικές χρήσιμες υποδείξεις για τη δημιουργία κωδικού είναι οι ακόλουθες:
    - Να αποτελείται από όσο το δυνατό περισσότερους χαρακτήρες, ώστε να είναι πιο δύσκολο να προβλεφθεί/υπολογιστεί. Πάντοτε να χρησιμοποιούνται τουλάχιστον 8 χαρακτήρες εκ των οποίων 2 από αυτούς να είναι αριθμοί.
    - Να χρησιμοποιούνται διαφορετικοί χαρακτήρες, αριθμοί, ειδικοί χαρακτήρες (!@#%^&*) και εναλλαγή κεφαλαίων και μικρών γραμμάτων.
    - Να αποφεύγεται η χρήση προσωπικών πληροφοριών (όνομα, αριθμός τηλεφώνου, διεύθυνση, ημερομηνία γέννησης, κ.λπ), καθώς είναι πολύ πιθανό κάποιος τρίτος να είναι σε θέση να τον μαντέψει.
    - Να αποφεύγονται κοινές λέξεις, γεωγραφικές ονομασίες ή ονόματα που περιλαμβάνονται στα λεξικά ή ονόματα που σχετίζονται με την επωνυμία ή τα προϊόντα της Επιχείρησης.
    - Ο κωδικός πρόσβασης να μην περιέχει μέρος ή ολόκληρο το όνομα χρήστη (username).
    - Να αποφεύγεται ο κωδικός πρόσβασης που επαναλαμβάνει τον ίδιο χαρακτήρα πολλές φορές ή που έχει ακολουθία αριθμών ή γραμμάτων ή μπορεί εύκολα να προβλεφθεί στο πληκτρολόγιο π.χ. 12345, qwerty ή στο αλφάβητο π.χ. abc, δηλαδή, να μη χρησιμοποιούνται χαρακτήρες που να είναι σε σειρά στο πληκτρολόγιο.
- Απαγορεύεται η χρήση των ίδιων συνθηματικών για συστήματα της Επιχείρησης και για συστήματα ή υπηρεσίες εκτός Επιχείρησης (πχ. οικιακοί υπολογιστές, προσωπικό hotmail/gmail/yahoo κτλ).
- Χρησιμοποιούνται διαφορετικά συνθηματικά για συστήματα με διαφορετικό βαθμό ευαισθησίας.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Για τους χρήστες που είναι συνδεδεμένοι με το Active Directory σχετικό είναι το ΠΑΡΑΡΤΗΜΑ IV

4.6.6. Απομακρυσμένη Πρόσβαση σε Ηλεκτρονικό Ταχυδρομείο

- Η σύνδεση με το δίκτυο της Επιχείρησης για λήψη/αποστολή ηλεκτρονικών μηνυμάτων εκτός του εργασιακού χώρου επιτρέπεται μόνο κατόπιν έγκρισης της Διοίκησης ή από τον Υπεύθυνο Ασφάλειας ΠΣ, ο οποίος έχει δώσει πρόσβαση με όνομα χρήστη και κωδικό πρόσβασης.
- Απαγορεύεται η απομακρυσμένη σύνδεση των εταιρειών, που παρέχουν λειτουργική υποστήριξη στα διάφορα Πληροφοριακά Συστήματα, στο Δίκτυο Δεδομένων χωρίς την εποπτεία από τον Υπεύθυνο Ασφάλειας ΠΣ.

4.6.7. Φυσική και Περιβαλλοντική Ασφάλεια

Ο όρος «Φυσική Ασφάλεια» αναφέρεται στα μέτρα που πρέπει να λαμβάνονται για την προστασία των πληροφοριών/δεδομένων, του μηχανογραφικού εξοπλισμού, του δικτυακού εξοπλισμού, των πληροφοριακών συστημάτων και της υποδομής που τα υποστηρίζει, από κινδύνους που προέρχονται από το φυσικό περιβάλλον.

Η φυσική ασφάλεια περιλαμβάνει μηχανισμούς ελέγχου φυσικής πρόσβασης (Physical Access Controls), πρόληψης και αντιμετώπισης καταστροφών από φυσικά αίτια (π.χ. σεισμούς, πυρκαγιές, ακραία καιρικά φαινόμενα κ.α.) και κακόβουλες ενέργειες (διάρρηξη/κλοπή, βανδαλισμός, τρομοκρατική ενέργεια, κλπ).

Για να αποφευχθεί η φυσική πρόσβαση από μη εξουσιοδοτημένα άτομα στους χώρους της Επιχείρησης όπου είναι εγκατεστημένος εξοπλισμός απαιτείται:

- Συμμόρφωση στις οδηγίες που αφορούν τους ελέγχους φυσικής πρόσβασης έτσι ώστε να περιορίζονται, να ελέγχονται και να καταγράφονται, αφ' ενός μεν η είσοδος και η έξοδος του προσωπικού και των επισκεπτών, αφ' ετέρου δε η μετακίνηση του μηχανογραφικού εξοπλισμού και των αποθηκευτικών μέσων.
- Οδήγηση των επισκεπτών/κοινό στους σωστούς χώρους. Ο κάθε εργαζόμενος είναι υπεύθυνος για τους δικούς του επισκέπτες και την κίνηση τους στο χώρο εργασίας. Οι επισκέπτες, σε καμία περίπτωση, δεν πρέπει να κινούνται στον εργασιακό χώρο χωρίς συνοδεία ή και να μένουν σε γραφεία χωρίς την παρουσία του υπάλληλου.
- Ασφαλής φύλαξη των αρχείων, εγγράφων και πληροφοριών, ιδιαίτερα των εμπιστευτικών καθώς και του φορητού εξοπλισμού (κινητά τηλέφωνα, φορητοί υπολογιστές, κλπ). Κατά τη μετακίνηση/μεταφορά τους, μέσω οχημάτων, θα πρέπει να μην είναι εκτεθειμένα σε περίοπτη θέση. Επιπλέον, τόσο τα εμπιστευτικά έγγραφα, όσο και ο εξοπλισμός δεν πρέπει να μένουν ανεπιτήρητα.
- Να μην είναι ορατή η οθόνη του Η/Υ από τους επισκέπτες/κοινό.
- Κατά την αποχώρηση του από το χώρο εργασίας, ο χρήστης θα πρέπει να σβήνει όλες τις συσκευές που έχει υπό την ευθύνη του (ηλεκτρονικός υπολογιστής, εκτυπωτής, κλπ.).

4.7. Διαχείριση Προβλημάτων

Ένας χρήστης μπορεί να υποψιαστεί ότι παραβιάζεται η ασφάλεια της πληροφορίας/ηλεκτρονικού υπολογιστή, όταν ξαφνικά, χωρίς να προηγηθεί οποιαδήποτε ενέργεια ή εγκατάσταση πρόσθετου

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

λογισμικού, λειτουργεί αργά, ή όταν αρχίσουν να εμφανίζονται περίεργα μηνύματα/προειδοποιήσεις στην οθόνη.

Σε τέτοιες περιπτώσεις ο χρήστης πρέπει να:

- Μην πανικοβληθεί.
- Μη σβήσει τον Η/Υ του.
- Σημειώσει το περιεχόμενο του προειδοποιητικού μηνύματος.
- Επικοινωνήσει με τον Ανώτερό του ή τη Διοίκηση της Εταιρείας.
- Ενεργήσει ανάλογα με τις οδηγίες που θα του δοθούν.
- Δώσει όλες τις απαραίτητες πληροφορίες που χρειάζονται, οι οποίες θα βοηθήσουν στην έρευνα και στην ανίχνευση του προβλήματος.

Είναι καθήκον όλων εργαζομένων να ενημερώνουν άμεσα τους Ανωτέρους τους ή τη Διοίκηση της Επιχείρησης σε περίπτωση που εντοπιστούν κακόβουλα προγράμματα (π.χ. ιοί), ύποπτες συμπεριφορές ή/και για οποιοδήποτε θέμα, το οποίο αφορά στην ασφάλεια της πληροφορίας/συστημάτων, κλπ.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

5

5. Πολιτική Προστασίας Προσωπικών Δεδομένων (Privacy)

5.1. Εισαγωγή

Η Επιχείρηση έχει την υποχρέωση να προστατεύει τα προσωπικά δεδομένα των πελατών της, καθώς κάθε άλλου προσώπου για το οποίο επεξεργάζεται πληροφορίες, και να διαφυλάσσει το απόρρητο στο βαθμό που αυτό εξαρτάται από τα ΠΣ.

Η πολιτική καθορίζει τον τρόπο με τον οποίο η Επιχείρηση και το προσωπικό της επιτυγχάνουν την τήρηση αυτών των υποχρεώσεων.

5.2. Σκοπός

Σκοπός της Πολιτικής Προστασίας Προσωπικών Δεδομένων είναι:

- Η συμμόρφωση της Επιχείρησης με τις νομικές και κανονιστικές υποχρεώσεις του Γενικού Κανονισμού ΕΕ/2016/679 "για την προστασία των φυσικών προσώπων έναντι επεξεργασίας των

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)".

- Η προστασία της ιδιωτικότητας των πελατών της Επιχείρησης.

5.3. Εμβέλεια

Η πολιτική αφορά τα μέλη του προσωπικού και τους συνεργάτες της Επιχείρησης που έχουν ή μπορεί να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα.

Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας ΠΣ.

5.4. Γενικές Αρχές

Συμμόρφωση με νομικές απαιτήσεις για προστασία προσωπικών δεδομένων

- Η Επιχείρηση προβαίνει σε όλες τις ενέργειες που απαιτούνται για τη τήρηση των υποχρεώσεών της που απορρέουν από το νομοθετικό και κανονιστικό πλαίσιο που αφορά την προστασία προσωπικών δεδομένων.

Υποχρέωση νομικής συμμόρφωσης προσωπικού

- Όλοι όσοι εργάζονται για την Επιχείρηση ή συνεργάζονται με αυτήν έχουν την υποχρέωση να συμβάλλουν στην προστασία των προσωπικών δεδομένων.

5.5. Οδηγίες και Κανόνες Ασφαλείας για την Προστασία Προσωπικών Δεδομένων

- Η Επιχείρηση επεξεργάζεται προσωπικά δεδομένα πελατών της μόνο μετά την ενημέρωσή τους και εφόσον έχει τη συγκατάθεση των πελατών της, όπως ο Κανονισμός GDPR ορίζει.
- Η Επιχείρηση ενημερώνει τους πελάτες της για την επεξεργασία των προσωπικών τους δεδομένων, μέσω της Πολιτικής Απορρήτου.
- Η Επιχείρηση επεξεργάζεται προσωπικά δεδομένα των υπαλλήλων της μόνο για λόγους που συνδέονται με την άσκηση της εργασίας τους.
- Η Επιχείρηση δεν μεταβιβάζει, ούτε αποκαλύπτει στοιχεία των πελατών της σε τρίτους, παρά μόνο κατόπιν δικαστικής ή εισαγγελικής εντολής ή όταν επιβάλλεται από το νόμο. Σε κάθε άλλη περίπτωση απαιτείται η ρητή συγκατάθεση του υποκειμένου.
- Η επεξεργασία δεδομένων που αφορούν πελάτες της Επιχείρησης γίνεται μόνο για τους σκοπούς που σχετίζονται με την παροχή υπηρεσιών σε αυτούς.
- Η συλλογή προσωπικών δεδομένων περιορίζεται μόνο στα δεδομένα που είναι απαραίτητα για την εκπλήρωση συμβατικών και νομικών υποχρεώσεων της Επιχείρησης.
- Η πρόσβαση του προσωπικού της Επιχείρησης στα προσωπικά δεδομένα των πελατών της περιορίζεται με βάση την αρχή ανάγκης γνώσης (need-to-know).
- Οι πελάτες της Επιχείρησης έχουν δικαίωμα πρόσβασης στις πληροφορίες που τους αφορούν. Για την άσκηση του δικαιώματος αυτού η Επιχείρηση μπορεί να ζητήσει την καταβολή εύλογου

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

αντίτιμου. Το αντίτιμο καταβάλλεται για να καλύψει έξοδα της Επιχείρησης, συνεπώς η Επιχείρηση δεν απολαμβάνει κέρδος από αυτό.

- Οι πελάτες έχουν το δικαίωμα να ζητήσουν τη διόρθωση προσωπικών τους στοιχείων που είναι αναληθή ή ανακριβή.
- Οι πελάτες έχουν το δικαίωμα να ζητήσουν τη διαγραφή των στοιχείων τους.
- Η φύλαξη προσωπικών αρχείων/εγγράφων/πληροφοριών στους Η/Υ ή εξυπηρετητές ή στο cloud της επιχείρησης απαγορεύεται.
- Όλοι οι εργαζόμενοι είναι υποχρεωμένοι όταν αποχωρούν από την εργασία τους, να σβήνουν όλες τις συσκευές που έχουν υπό την ευθύνη τους, είτε είναι Η/Υ, είτε εκτυπωτής κτλ.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

6

6.Πολιτική Αναδόχων και Συνεργατών

6.1. Εισαγωγή

Οι δραστηριότητες των συνεργατών της Επιχείρησης, είτε πρόκειται για φυσικά πρόσωπα είτε για εταιρείες που αναλαμβάνουν διάφορες εργασίες, όπως εργασίες ανάπτυξης και συντήρησης συστημάτων, εκτυπωτικές εργασίες κλπ., καθώς και των προμηθευτών υπηρεσιών, ειδικά όσων έχουν πρόσβαση σε ιδιωτικούς διακομιστές (ftp), μπορεί να θέσουν σε κίνδυνο την εφαρμογή της Πολιτικής Ασφάλειας ΠΣ της Επιχείρησης.

Η Επιχείρηση διατηρεί την ευθύνη απέναντι στο Νόμο για την παραβίαση του απορρήτου των επικοινωνιών ή την κατάχρηση των προσωπικών δεδομένων των πελατών όταν αυτή προέλθει από συνεργάτες της Επιχείρησης ή από αναδόχους εργασιών. Για αυτούς τους λόγους πρέπει να διασφαλίζεται ότι αυτοί οι ανάδοχοι και οι συνεργάτες συμμορφώνονται και εφαρμόζουν τα όσα ορίζει η Πολιτική Ασφάλειας ΠΣ.

6.2. Σκοπός

Σκοπός της Πολιτικής Αναδόχων και Συνεργατών είναι:

- Η αποτροπή πιθανών επιβλαβών συμβάντων που μπορεί να προκύψουν από τις δραστηριότητες των αναδόχων εργασιών και των συνεργατών της Επιχείρησης.
- Να διασφαλιστεί ότι προστατεύονται τα προσωπικά δεδομένα των πελατών της Επιχείρησης.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

6.3. Γενικές Αρχές

Υποχρεώσεις αναδόχων και συνεργατών

- Οι συνεργάτες της Επιχείρησης και οι ανάδοχοι εργασιών έχουν τις ίδιες υποχρεώσεις αναφορικά με την ασφάλεια ΠΣ που έχει και το προσωπικό της Επιχείρησης.

Προστασία ΠΣ από ενέργειες αναδόχων και συνεργατών

- Η Επιχείρηση αναγνωρίζει τους κινδύνους που προέρχονται από τις δραστηριότητες των συνεργατών της και των αναδόχων εργασιών και λαμβάνει όλα τα μέτρα ώστε να τους περιορίσει.

6.4. Οδηγίες και κανόνες ασφάλειας

6.4.1. Υποχρεώσεις αναδόχων και συνεργατών

- Οι ανάδοχοι εργασιών και οι συνεργάτες της Επιχείρησης οφείλουν να γνωρίζουν και να εφαρμόζουν την Πολιτική Ασφάλειας ΠΣ της Επιχείρηση. Για το προσωπικό των αναδόχων που εκτελούν εργασίες στις εγκαταστάσεις ή/και στα ΠΣ της Επιχείρησης ισχύουν οι ίδιοι κανόνες με το προσωπικό της Επιχείρησης.
- Οι ανάδοχοι εργασιών και οι συνεργάτες της Επιχείρησης οφείλουν να αναφέρουν κάθε περιστατικό που μπορεί να θέσει σε κίνδυνο τα ΠΣ της Επιχείρησης.
- Οι ανάδοχοι εργασιών και οι συνεργάτες της Επιχείρησης οφείλουν να διατηρούν την εμπιστευτικότητα των δεδομένων στα οποία αποκτούν πρόσβαση.
- Οι ανάδοχοι εργασιών και οι συνεργάτες της Επιχείρησης απαγορεύεται να αποκαλύπτουν πληροφορίες ή άλλα στοιχεία που συνδέονται με τα προσωπικά δεδομένα χρηστών και πελατών.

6.4.2. Συμβάσεις

- Οι συμβάσεις έργων που σχετίζονται με τη λειτουργία των ΠΣ περιλαμβάνουν όρους που εξασφαλίζουν συμβατικά και τεχνικά την τήρηση της Πολιτικής Ασφάλειας ΠΣ της Επιχείρησης.
- Οι συμβάσεις έργων που σχετίζονται με τη λειτουργία των ΠΣ της Επιχείρησης περιλαμβάνουν ρήτρες σε περίπτωση μη συμμόρφωσης με την Πολιτική Ασφάλειας ΠΣ της Επιχείρησης.
- Για την πρόσβαση σε προσωπικά δεδομένα πελατών απαιτείται η λήψη άδειας από την Διοίκηση.
- Ο Υπεύθυνος Ασφάλειας ΠΣ οφείλει να ελέγχει και να γνωμοδοτεί για την επάρκεια των όρων της σύμβασης σε σχέση με την ασφάλεια ΠΣ, όπως επίσης και για τη δυνατότητα του αναδόχου ή συνεργάτη να ανταποκριθεί στις απαιτήσεις ασφάλειας που θέτει η Επιχείρηση.
- Οι όροι που αφορούν την τήρηση της Πολιτικής Ασφάλειας ΠΣ περιλαμβάνονται και στις προκηρύξεις των έργων.
- Τα άτομα που πραγματοποιούν εργασίες στα ΠΣ της Επιχείρησης καταγράφονται και η ταυτότητά τους ελέγχεται.
- Εξωτερικά συνεργεία συντήρησης, επισκευών και καθαρισμού συνοδεύονται διαρκώς από άτομα της Επιχείρησης όταν βρίσκονται σε ευαίσθητους χώρους.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

7

7. Πολιτική Προστασίας Πληροφοριακών Συστημάτων

7.1. Εισαγωγή

Η Πολιτική Προστασίας ΠΣ προδιαγράφει τα μέσα και τις διαδικασίες με τα οποία διασφαλίζονται τα ΠΣ της Επιχείρησης. Η Πολιτική αναφέρεται κυρίως στα τεχνικά μέσα και στις διαδικασίες που εφαρμόζουν οι διαχειριστές-μηχανικοί της Επιχείρησης.

Με την πολιτική αυτή διασφαλίζεται ότι υφίσταται και λειτουργεί ένα επαρκές σύστημα ασφάλειας, ικανό να επιτύχει τους σχετικούς με την ασφάλεια στόχους, όπως αυτοί περιγράφονται στην Πολιτική Ασφάλειας ΠΣ.

7.2. Σκοπός

Σκοπός της Πολιτικής Προστασίας ΠΣ είναι:

- Να προδιαγράψει τα απαιτούμενα μέσα και τις κατάλληλες διαδικασίες για την προστασία των ΠΣ από εκούσιες ή ακούσιες απειλές.
- Να διασφαλίσει ότι τα τεχνικά μέτρα προστασίας επαρκούν για την εφαρμογή της Πολιτικής Ασφάλειας ΠΣ.
- Να διασφαλίσει ότι η Επιχείρηση έχει τα τεχνικά μέσα που απαιτούνται για να ανταποκριθεί στις νομικές, κανονιστικές και συμβατικές υποχρεώσεις της.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

7.3. Εμβέλεια

Η Πολιτική Προστασίας ΠΣ αφορά το σύνολο των συστημάτων που υποστηρίζουν τις δραστηριότητες της Επιχείρησης ή που μπορεί να επηρεάσουν τις δραστηριότητές της.
Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας ΠΣ.

7.4. Γενικές Αρχές

Περιγράφονται τα μέτρα ασφαλείας που εφαρμόζονται από τον οργανισμό ή την επιχείρηση. Τα μέτρα ασφαλείας μπορούν να εντάσσονται στις παρακάτω τρεις κύριες κατηγορίες:

7.4.1. Ανάπτυξη ή προμήθεια συστημάτων και εγκατάστασή τους

- Όλες οι προμήθειες συστημάτων βασίζονται σε προδιαγραφές, οι οποίες λαμβάνουν υπόψη και τα ζητήματα ασφάλειας.
- Οι προδιαγραφές ασφάλειας ελέγχονται από τον Υπεύθυνο Ασφάλειας ΠΣ, καθώς και από τη διεύθυνση που θα αναλάβει τη διαχείριση των συστημάτων έπειτα από την εγκατάστασή τους.
- Όλα τα συστήματα ελέγχονται και τίθενται σε δοκιμαστική λειτουργία πριν τεθούν σε παραγωγική λειτουργία.
- Όλα τα συστήματα, ανεξαρτήτως μεγέθους και πολυπλοκότητας, που αναπτύσσονται από στελέχη της Επιχείρησης ενσωματώνουν επαρκείς μηχανισμούς ασφάλειας. Ιδιαίτερη προσοχή αποδίδεται στην αυθεντικοποίηση (authentication) και τον έλεγχο πρόσβασης των χρηστών.

7.4.2. Έλεγχος πρόσβασης

- Η απονομή δικαιωμάτων πρόσβασης στα ΠΣ της Επιχείρησης ακολουθεί την αρχή ανάγκης γνώσης (need-to-know).
- Τα δικαιώματα πρόσβασης που παρέχονται σε κάθε πρόσωπο ή διεργασία λογισμικού (software process) καταγράφονται και τηρείται σχετικός κατάλογος.
- Η πρόσβαση στα ΠΣ ελέγχεται από κατάλληλους μηχανισμούς ελέγχου πρόσβασης.
- Η Επιχείρηση τηρεί σαφείς διαδικασίες για τη προσθήκη νέων χρηστών, τις μεταβολές στα επίπεδα πρόσβασης των χρηστών, την πρόσβαση σε κρυπτογραφικούς μηχανισμούς, κλειδιά κλπ.
- Η Επιχείρηση προδιαγράφει τους μηχανισμούς ταυτοποίησης και ελέγχου πρόσβασης που εφαρμόζει.
- Οι μηχανισμοί ελέγχου πρόσβασης καλύπτουν τα δεδομένα σε όλες τις μορφές τους, συμπεριλαμβανομένων των μαγνητικών ή οπτικών μέσων μεταφοράς, τα εφεδρικά αντίγραφα δεδομένων (back up), τα δεδομένα που μεταβιβάζονται μέσω δικτύων, δεδομένα σε έντυπη μορφή κλπ.
- Οι μηχανισμοί ελέγχου πρόσβασης διασφαλίζουν ότι υπάρχει δυνατότητα ταυτοποίησης του ατόμου που πραγματοποίησε μία ενέργεια. Η αρχή αυτή ισχύει τόσο για τους χρήστες, όσο και για τους διαχειριστές (μηχανικούς, τεχνικούς κλπ.).
- Οι διαχειριστές των συστημάτων δεν έχουν τη δυνατότητα να παρακάμψουν τους μηχανισμούς ελέγχου πρόσβασης χωρίς εξουσιοδότηση και με την προϋπόθεση ότι η ενέργειά τους αυτή καταγράφεται και ελέγχεται.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

- Οι χρήστες λαμβάνουν οδηγίες για την επιλογή και διαχείριση των συνθηματικών τους.
- Η αυστηρότητα των μηχανισμών ελέγχου πρόσβασης είναι αντίστοιχη της διαβάθμισης των δεδομένων.

7.4.3. Αντιμετώπιση Περιστατικών και Διασφάλιση Συνέχειας Λειτουργίας

- Όλα τα ύποπτα περιστατικά αναφέρονται στον Υπεύθυνο Ασφάλειας ΠΣ. Για αυτόν το σκοπό αναπτύσσονται διαδικασίες που διευκολύνουν την αναφορά τους.
- Το προσωπικό ενθαρρύνεται να αναφέρει ύποπτα περιστατικά, έστω και εάν υπάρχουν περιορισμένες πιθανότητες να αφορούν πραγματική απειλή για τα ΠΣ της Επιχείρησης.
- Όλα τα ύποπτα περιστατικά διερευνώνται.
- Σε περιπτώσεις όπου υπάρχουν ποινικά αδικήματα τα στοιχεία διαβιβάζονται στις εισαγγελικές αρχές.
- Η γνώση που προκύπτει από τη διερεύνηση των ύποπτων περιστατικών αξιοποιείται για τη βελτίωση της ασφάλειας των ΠΣ.
- Οι διαδικασίες συλλογής στοιχείων είναι διαφανείς και δεν αφήνουν περιθώρια αμφισβήτησης των στοιχείων.
- Αναπτύσσεται και εφαρμόζεται σχέδιο συνέχειας λειτουργίας (business continuity plan).
- Το σχέδιο συνέχειας λειτουργίας βασίζεται στις απαιτήσεις διαθεσιμότητας των ΠΣ και ακεραιότητας των πληροφοριών.
- Το σχέδιο συνέχειας λειτουργίας λαμβάνει υπόψη την πιθανότητα καταστροφικών γεγονότων που μπορεί να θέσουν εκτός λειτουργίας ολόκληρες εγκαταστάσεις (πχ. σεισμός, πυρκαγιά, τρομοκρατική επίθεση κλπ.).

7.4.4. Χρήση κρυπτογραφικών μεθόδων

- Χρησιμοποιούνται κρυπτογραφικές μέθοδοι που ακολουθούν διεθνή πρότυπα.
- Δεν χρησιμοποιούνται κρυπτογραφικές μέθοδοι που δεν έχουν τεθεί σε δημόσιο έλεγχο.
- Επιλέγονται κρυπτογραφικές μέθοδοι ανάλογα με την εφαρμογή για την οποία χρησιμοποιούνται.
- Η χρήση κρυπτογραφικών μεθόδων γίνεται σύμφωνα με το νομοθετικό και κανονιστικό πλαίσιο που ισχύει στη χώρα.
- Το μήκος του κλειδιού έχει επαρκές μέγεθος και έχει εγκριθεί από τον Υπεύθυνο Ασφάλειας ΠΣ.
- Η διαχείριση των κλειδιών εξασφαλίζει αφενός ότι δεν παραβιάζεται η πολιτική ελέγχου πρόσβασης και αφετέρου ότι δεν υφίσταται κίνδυνος απώλειας των δεδομένων λόγω απώλειας των κλειδιών.

7.4.5. Ασφάλεια εγκαταστάσεων

- Οι εγκαταστάσεις που επιλέγονται για να στεγάσουν κρίσιμες λειτουργίες των ΠΣ παρέχουν επαρκή προστασία από κλοπή, τρομοκρατική ενέργεια, βανδαλισμούς, φωτιά, πλημμύρα, σεισμό, ή άλλες φυσικές καταστροφές και κινδύνους.
- Οι εγκαταστάσεις είναι κατάλληλες ώστε να διασφαλίσουν την απρόσκοπτη λειτουργία του εξοπλισμού.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

- Χρησιμοποιούνται σύγχρονες τεχνολογίες ελέγχου πρόσβασης (πχ. proximity cards), προκειμένου να διασφαλίζεται ο επαρκής έλεγχος σε συνδυασμό με την ευκολία πρόσβασης και διακίνησης των εξουσιοδοτημένων προσώπων.

7.4.6. Προστασία συστημάτων

- Ο σχεδιασμός προστασίας του λογισμικού προστατεύει το λογισμικό εφαρμογών, το λογισμικό συστήματος και τα εργαλεία ανάπτυξης.
- Τα δίκτυα διαχωρίζονται ανάλογα με τη διαβάθμιση των δεδομένων που διακινούνται σε αυτά.
- Τα δίκτυα προστατεύονται τόσο από εσωτερικές, όσο και από εξωτερικές απειλές.
- Η προστασία των δικτύων περιλαμβάνει και την προστασία του δικτυακού εξοπλισμού.
- Εγκαθίστανται αποτελεσματικοί μηχανισμοί για την προστασία των ΠΣ της Επιχείρησης από ιομορφικό λογισμικό.
- Η χρήση του ηλεκτρονικού ταχυδρομείου και του Διαδικτύου ελέγχεται, ώστε να μην εκτίθενται σε κινδύνους τα ΠΣ της Επιχείρησης.
- Η ανεπιθύμητη ηλεκτρονική αλληλογραφία (spam) περιορίζεται.
- Ο βασικός εξοπλισμός ΤΠΕ προστατεύεται, τόσο φυσικά, όσο και λογικά.

7.5. Οργανωτικά μέτρα ασφαλείας

7.5.1. Ορισμός Υπεύθυνου Ασφαλείας

Η Επιχείρηση έχει ορίσει διακριτή θέση υπεύθυνου ασφαλείας, ο οποίος έχει, τουλάχιστον, την επίβλεψη και τον έλεγχο της εφαρμογής της πολιτικής ασφαλείας και των μέτρων ασφαλείας.

7.5.2. Καταστροφή δεδομένων και αποθηκευτικών μέσων

Α) Διαδικασίες καταστροφής δεδομένων

Πριν από την καταστροφή εντύπων ή ηλεκτρονικών αρχείων που περιέχουν προσωπικά δεδομένα θα πρέπει να λαμβάνονται τα κατάλληλα μέτρα ώστε να διασφαλίζεται η πλήρης και μόνιμη διαγραφή των δεδομένων αυτών. Ειδικότερα, θα πρέπει να ακολουθούνται κατ' ελάχιστον όσα προβλέπονται στην Οδηγία 1/2005 της Αρχής για την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας.

Ο υπεύθυνος επεξεργασίας οφείλει να διαθέτει συγκεκριμένη γραπτή διαδικασία για την καταστροφή των δεδομένων, τόσο όταν πρόκειται για προγραμματισμένη μαζική καταστροφή δεδομένων, όσο και όταν πρόκειται για καταστροφή δεδομένων σε καθημερινή βάση (π.χ. με χρήση καταστροφέων εγγράφων) και να ενημερώνει σχετικά τους υπαλλήλους του.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

7.6. Τεχνικά μέτρα ασφαλείας

7.6.1. Έλεγχος πρόσβασης

Α) Διαχείριση λογαριασμών χρηστών

Ο υπεύθυνος επεξεργασίας πρέπει να υιοθετήσει συγκεκριμένες διαδικασίες για τη διαχείριση των λογαριασμών των χρηστών, οι οποίες πρέπει να περιλαμβάνουν κατ' ελάχιστο διαδικασίες για την προσθήκη, μεταβολή ιδιοτήτων και διαγραφή λογαριασμού. Πρέπει να αποδίδεται διαφορετικός λογαριασμός πρόσβασης σε κάθε χρήστη.

Β) Μηχανισμοί ελέγχου πρόσβασης

Πρέπει να αναπτυχθούν μηχανισμοί που να μην επιτρέπουν προσβάσεις σε πόρους/εφαρμογές/αρχεία από μη εξουσιοδοτημένους χρήστες: ουσιαστικά, πρέπει να υπάρχουν κατάλληλα μέτρα που να εξασφαλίζουν την εγγυημένα ορθή ταυτοποίηση και αυθεντικοποίηση των χρηστών, ενώ ταυτοχρόνως πρέπει να γίνεται σε τεχνικό επίπεδο συγκεκριμένη εκχώρηση δικαιωμάτων/εξουσιοδοτήσεων σε κάθε χρήστη.

Γ) Διαχείριση συνθηματικών

Ο υπεύθυνος επεξεργασίας οφείλει να υιοθετήσει συγκεκριμένη πολιτική διαχείρισης των συνθηματικών των χρηστών, η οποία να περιλαμβάνει τουλάχιστον κανόνες αποδοχής για το ελάχιστο μήκος και επιτρεπτούς χαρακτήρες των συνθηματικών (πολυπλοκότητα συνθηματικού), την ιστορικότητα του συνθηματικού και τη συχνότητα αλλαγής του.

Τα συνθηματικά δεν πρέπει να είναι κάπου καταγεγραμμένα στην πραγματική τους μορφή (ούτε σε φυσικό ούτε σε ηλεκτρονικό αρχείο). Εάν τα συνθηματικά διατηρούνται ηλεκτρονικά στο πλαίσιο της διαδικασίας ταυτοποίησης-αυθεντικοποίησης των χρηστών, τότε πρέπει να είναι σε μη αναγνώσιμη μορφή από την οποία δεν πρέπει να είναι εφικτή η ανάκτηση της αρχικής τους μορφής. Επίσης, οι χρήστες πρέπει να υποχρεώνονται να αλλάζουν οι ίδιοι το (προκαθορισμένο) συνθηματικό που τους ανατίθεται εξαρχής, καθώς επίσης και να υποχρεώνονται να αλλάζουν το συνθηματικό τους ανά τακτά χρονικά διαστήματα (οπωσδήποτε εντός διαστήματος μικρότερου του ενός έτους).

Δ) Μη επιτυχημένες προσπάθειες πρόσβασης

Πρέπει να υπάρχουν κατάλληλοι μηχανισμοί ώστε να απαγορεύεται η πρόσβαση σε έναν εξουσιοδοτημένο χρήστη, μετά από ένα πλήθος επαναλαμβανομένων αποτυχημένων αιτήσεων πρόσβασης (για παράδειγμα, υποβολή λανθασμένων συνθηματικών). Για έναν τέτοιο χρήστη, πρέπει να επανεξετάζεται η εξουσιοδότησή του για να έχει δικαίωμα πρόσβασης.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Ε) Αδρανοποιημένος υπολογιστής

Μέτρα πρέπει να ληφθούν προς αποφυγή περιπτώσεων όπου θα δύναται κάποιος να έχει εύκολα πρόσβαση οποιουδήποτε τύπου σε προσωπικά δεδομένα, λόγω ενός ανοιχτού υπολογιστή, ο οποίος μένει χωρίς επίβλεψη (έστω και για λίγα λεπτά). Προς αυτή την κατεύθυνση μπορούν ενδεικτικά να αναπτυχθούν διαδικασίες αυτόματης αποσύνδεσης (μετά από ένα εύλογο χρονικό διάστημα αδράνειας) ή/και ενεργοποίηση της προφύλαξης οθόνης (screen saver) του υπολογιστή – για την απενεργοποίηση της οποίας θα απαιτείται χρήση συνθηματικού.

7.6.2. Διαμόρφωση υπολογιστών

Α) Προστασία από κακόβουλο λογισμικό

Πρέπει να υπάρχει προστασία από κακόβουλο λογισμικό όλων των υπολογιστών (τόσο των προσωπικών υπολογιστών των υπαλλήλων όσο και των διακομιστών (servers)) που τηρούν ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα. Αυτό μπορεί να επιτευχθεί (πέραν της σωστής χρήσης αυτών από τους υπαλλήλους) με αντιβιοτικά προγράμματα (antivirus), καθώς και με χρήση προγραμμάτων τειχών ασφαλείας (firewall). Τόσο το antivirus όσο και το firewall πρέπει να διαθέτουν ανά πάσα στιγμή τις πλέον πρόσφατες ενημερώσεις. Επιπλέον, στο λειτουργικό σύστημα των υπολογιστών (εφόσον είναι συνδεδεμένοι στο Διαδίκτυο) πρέπει να εγκαθίστανται ανά τακτά διαστήματα ενημερώσεις ασφαλείας.

Β) Ρυθμίσεις υπολογιστών

Δεν πρέπει να επιτρέπονται ενέργειες απλών χρηστών στους υπολογιστές οι οποίες επηρεάζουν τη συνολική τους διαμόρφωση (π.χ. απενεργοποίηση αντιβιοτικών προγραμμάτων, εγκατάσταση νέων προγραμμάτων ή αλλαγή ρυθμίσεων υπαρχόντων, κ.λπ.). Πρέπει να γίνεται περιοδικός έλεγχος του εγκατεστημένου λογισμικού για τον τυχόν εντοπισμό προγραμμάτων που έχουν εγκατασταθεί εκτός των εγκεκριμένων διαδικασιών.

Γ) Υπολογιστές-διακομιστές

Σε περίπτωση που κάποιος υπολογιστής χρησιμοποιείται σαν κεντρικός διακομιστής (server) για άλλους υπολογιστές, τότε δεν θα πρέπει να μπορεί να χρησιμοποιείται ως σταθμός εργασίας από κάποιον χρήστη.

Δ) Σύνδεση αποσπώμενων μέσων

Οι ηλεκτρονικοί υπολογιστές που χρησιμοποιούνται από τους τελικούς χρήστες δεν πρέπει να διαθέτουν δυνατότητα εξαγωγής δεδομένων με τη χρήση αποσπώμενων μέσων (π.χ. USB, CD/DVD) – εκτός αν υπάρχει έγκριση από τον Υπεύθυνο Ασφαλείας (ή άλλης μορφής έγκριση, μέσω διαδικασίας που προβλέπεται στην πολιτική ασφαλείας).

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Ε) Υπολογιστές με πρόσβαση στο Διαδίκτυο

Δεν πρέπει να αποθηκεύονται δεδομένα προσωπικού χαρακτήρα σε υπολογιστές που έχουν σύνδεση με το διαδίκτυο (εκτός αν κάτι τέτοιο είναι απολύτως απαραίτητο στο πλαίσιο του ρόλου/αρμοδιοτήτων που έχουν ανατεθεί στο χρήστη του υπολογιστή).

7.6.3. Αρχεία καταγραφής (log files)

Α) Τήρηση και έλεγχος αρχείων καταγραφής

Στα κρίσιμα συστήματα, θα πρέπει να υπάρχουν διαδικασίες για την τήρηση και τον έλεγχο των αρχείων καταγραφής όλων των ενεργειών (log files) των χρηστών, συμπεριλαμβανομένων και των ενεργειών των διαχειριστών των συστημάτων, καθώς και των συμβάντων ασφαλείας. Πρέπει να διασφαλίζεται η προστασία και η ακεραιότητα των αρχείων αυτών.

Στα αρχεία αυτά δύναται να έχουν πρόσβαση ο υπεύθυνος ασφαλείας, οι διαχειριστές συστημάτων και όποια άλλα μέλη του προσωπικού είναι επιφορτισμένα με αρμοδιότητες διαχείρισης περιστατικών ασφαλείας κατόπιν έγγραφης εξουσιοδότησης.

Η πρόσβαση στα αρχεία καταγραφής πρέπει επίσης να καταγράφεται και να υπόκειται στους ίδιους περιορισμούς με τα υπόλοιπα αρχεία καταγραφής.

Β) Ειδικές ενέργειες που πρέπει να καταγράφονται

Πρέπει να ληφθεί μέριμνα ώστε στα αρχεία καταγραφής ενεργειών να τηρούνται οπωσδήποτε, κατ' ελάχιστο, τα εξής: το αναγνωριστικό του χρήστη που αιτήθηκε την προσπέλαση δεδομένων προσωπικού χαρακτήρα, η ημερομηνία και ώρα του σχετικού αιτήματος, το σύστημα μέσω του οποίου αιτήθηκε την πρόσβαση (υπολογιστής, πρόγραμμα λογισμικού, κ.λπ.), καθώς και αν τελικά προσπέλασε τα αρχεία που αιτήθηκε. Επίσης, πρέπει να καταγράφονται και τα αιτήματα εκτύπωσης αρχείων με προσωπικά δεδομένα, καθώς και οι αλλαγές σε κρίσιμα αρχεία του συστήματος ή στα δικαιώματα των χρηστών. Επίσης, πρέπει να τηρούνται στοιχεία που αφορούν τις προσπάθειες μη εξουσιοδοτημένης πρόσβασης και τις αλλαγές στην παραμετροποίηση εφαρμογών και συστημάτων, τον προκαθορισμό κρίσιμων γεγονότων (events), η καταγραφή των οποίων θα επιβλέπεται άμεσα από τον υπεύθυνο ασφαλείας και τους διαχειριστές των συστημάτων και γενικότερα κάθε ενέργεια η οποία μπορεί να υποδηλώνει διενέργεια επίθεσης, όπως προσπάθειες καταγραφής των προσφερόμενων υπηρεσιών του συστήματος (port scanning).

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Γ) Διαγραφή αρχείων καταγραφής

Δεν θα πρέπει να υφίσταται δυνατότητα διαγραφής των αρχείων καταγραφής του συστήματος από ένα μόνο άτομο. Τέτοια διαγραφή θα πρέπει να γίνεται με την παρουσία 2 τουλάχιστον ατόμων, τα οποία θα έχουν διαφορετικούς ρόλους (π.χ. υπεύθυνος ασφαλείας + διοικητικός διευθυντής).

7.6.4. Ασφάλεια επικοινωνιών

Α) Έλεγχος δικτυακών συσκευών

Πρέπει να εξασφαλίζεται επαρκής έλεγχος των συνδεόμενων στο δίκτυο συσκευών (ως προς την πρόσβαση σε αυτές αλλά και τη χρήση τους).

Β) Απομακρυσμένη πρόσβαση

Ο υπεύθυνος επεξεργασίας πρέπει να υιοθετήσει συγκεκριμένη διαδικασία για τη διαχείριση της απομακρυσμένης πρόσβασης σε συστήματα (π.χ. από εταιρείες συντήρησης) μέσω ασφαλών καναλιών με δυνατή ταυτοποίηση/αυθεντικοποίηση και κρυπτογράφηση. Προς τούτο, επισημαίνεται ιδιαίτερα ότι οι τεχνολογίες απομακρυσμένης πρόσβασης (π.χ. Remote Desktop, VNC, ασύρματη σύνδεση, κ.λπ.) πρέπει να επιτρέπονται μόνο σε εξουσιοδοτημένα πρόσωπα για τα οποία είναι απόλυτα απαραίτητες στο πλαίσιο των αρμοδιοτήτων τους. Συνεπώς, η απομακρυσμένη πρόσβαση πρέπει να γίνεται υπό την εποπτεία και έλεγχο του υπευθύνου επεξεργασίας (π.χ. των διαχειριστών ή/και του υπευθύνου ασφαλείας) και να καταγράφεται.

Γ) Κανάλι επικοινωνίας

Πρέπει να εξασφαλίζεται ότι η επικοινωνία μεταξύ υπολογιστών/κόμβων γίνεται μέσω επαρκώς ασφαλούς καναλιού επικοινωνίας (π.χ. με χρήση κρυπτογράφησης ή ιδιωτικών γραμμών ελεγχόμενης φυσικής πρόσβασης).

Δ) Πρωτόκολλα δικτύου

Πρέπει να αποφεύγεται η χρήση ευπαθών ως προς την ασφάλεια πρωτοκόλλων όπως FTP, telnet (όπου δεν γίνεται κρυπτογράφηση) και, όταν υπηρεσίες τέτοιων πρωτοκόλλων είναι αναγκαίες, να γίνεται χρήση των αντίστοιχων ασφαλών (όπως, για παράδειγμα, SFTP, SSH).

Ε) Περιμετρική ασφάλεια

Πρέπει να υπάρχει διαδικασία για τον επαρκή έλεγχο των δικτυακών συνδέσεων του εσωτερικού δικτύου του υπευθύνου επεξεργασίας από και προς το διαδίκτυο ή άλλα εξωτερικά, μη έμπιστα, δίκτυα όπως μέσω

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

του σημείου ελέγχου της περιμέτρου (firewall). Οι συνδέσεις που ενεργοποιούνται μέσω του firewall και οι υπηρεσίες που εξυπηρετούν πρέπει να εγκρίνονται από τον υπεύθυνο ασφαλείας. Πρέπει, επίσης, να τηρείται επικαιροποιημένος κατάλογος με τις εγκεκριμένες συνδέσεις από και προς το δίκτυο του υπευθύνου επεξεργασίας και τις υπηρεσίες που εξυπηρετούν.

7.6.5. Αποσπώμενα μέσα αποθήκευσης

Α) Χρήση κρυπτογράφησης

Πρέπει να υπάρχουν διαδικασίες για την αποτελεσματική κρυπτογράφηση (επιλογή σύγχρονων και ισχυρών αλγορίθμων κρυπτογράφησης, κατάλληλο μέγεθος κλειδιών και τεχνικές διαχείρισης αυτών, κ.λπ.) αρχείων με προσωπικά δεδομένα, ιδίως ευαίσθητα σύμφωνα με το άρθρο 2 εδ. β) ν.2472/1997, που τηρούνται σε φορητά αποθηκευτικά μέσα (π.χ. USB δίσκους κ.ο.κ.), αφού για αυτές τις περιπτώσεις ο κίνδυνος διαρροής δεδομένων αυξάνεται.

7.6.6. Ασφάλεια λογισμικού

Α) Σχεδιασμός εφαρμογών

Ο σχεδιασμός των εφαρμογών που χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων πρέπει να πραγματοποιείται λαμβάνοντας υπόψη τις βασικές αρχές της προστασίας προσωπικών δεδομένων και της ιδιωτικότητας (privacy by design). Ως εκ τούτου, οι εφαρμογές πρέπει, σύμφωνα με το άρθρο 4 του ν. 2472/1997, να ακολουθούν την αρχή της ελαχιστοποίησης των δεδομένων (data minimization), καθώς και της ποιότητας των δεδομένων και να περιλαμβάνουν τη δυνατότητα της διαγραφής δεδομένων μετά το χρονικό διάστημα που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Επίσης, πρέπει να επιτρέπουν την υλοποίηση όλων των απαιτούμενων τεχνικών μηχανισμών ασφαλείας για την προστασία των δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

Β) Ασφαλής ανάπτυξη εφαρμογών

Σε περίπτωση ανάπτυξης εφαρμογών, είτε εσωτερικά στον οργανισμό είτε από εξωτερικό συνεργάτη, θα πρέπει να προβλέπεται διαδικασία ασφαλούς υλοποίησης λογισμικού, ώστε να εντοπισθούν τυχόν ευπάθειες αυτού ως προς την ασφάλεια προτού αυτό μεταβεί σε λειτουργική φάση. Στις περιπτώσεις όπου η ανάπτυξη των εφαρμογών γίνεται από εξωτερικό συνεργάτη, θα πρέπει να υπάρχουν προδιαγραφές ασφαλείας της εφαρμογής στο έγγραφο περιγραφής απαιτήσεων λογισμικού, το οποίο εμπεριέχεται στη σύμβαση με τον εκάστοτε ανάδοχο.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Γ) Προστασία αρχείων λειτουργικών συστημάτων

Τα λειτουργικά αρχεία των συστημάτων (system files), τα δεδομένα ελέγχου συστημάτων (system test data), καθώς και ο πηγαίος κώδικας (source code) των προγραμμάτων λογισμικού πρέπει να ελέγχονται και να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση.

7.6.7. Διαχείριση αλλαγών

Α) Πολιτική διαχείρισης αλλαγών

Ο υπεύθυνος επεξεργασίας πρέπει να ορίσει σαφή πολιτική διαχείρισης όλων των αλλαγών που πραγματοποιούνται στα πληροφοριακά συστήματα, η οποία να περιέχει κατ' ελάχιστον: καταγραφή των αιτημάτων αλλαγής, καθορισμό των ρόλων που έχουν δικαίωμα έγκρισης των αλλαγών, καθορισμό των κριτηρίων αποδοχής της αλλαγής και χρονοδιάγραμμα υλοποίησης.

Β) Περιβάλλον δοκιμών

Θα πρέπει να γίνεται δοκιμή των ενημερώσεων λογισμικού, τόσο σε επίπεδο επιμέρους εφαρμογών όσο και σε επίπεδο λειτουργικού συστήματος, σε δοκιμαστικό περιβάλλον. Προαιρετικά, ο υπεύθυνος επεξεργασίας μπορεί να εφαρμόσει κεντρική διαχείριση όλων των ενημερώσεων λογισμικού.

Η ανάπτυξη λογισμικού πρέπει να γίνεται σε δοκιμαστικό περιβάλλον, το οποίο να είναι απομονωμένο από το παραγωγικό σύστημα και επικαιροποιημένο. Κατά την ανάπτυξη ή αναβάθμιση λογισμικού και τη δοκιμή του θα πρέπει να χρησιμοποιούνται δοκιμαστικά και όχι πραγματικά δεδομένα ή δεδομένα του παραγωγικού συστήματος, εκτός εάν κάτι τέτοιο είναι απολύτως απαραίτητο και δεν υπάρχει εναλλακτική λύση. Αν είναι αναγκαίο μπορούν να χρησιμοποιηθούν πραγματικά δεδομένα σε ανωνυμοποιημένη μορφή ή διαφορετικά πρέπει να περιορίζονται στα απολύτως απαραίτητα για τους σκοπούς του ελέγχου.

7.7. Μέτρα φυσικής ασφαλείας

7.7.1. Έλεγχος φυσικής πρόσβασης

Α) Φυσική πρόσβαση σε εγκαταστάσεις και computer room

Πρέπει να υπάρχουν τα κατάλληλα μέτρα ελέγχου φυσικής πρόσβασης στους κρίσιμους χώρους όπου βρίσκεται ο φυσικός εξοπλισμός (συμπεριλαμβανομένης τηλεπικοινωνιακής και δικτυακής καλωδίωσης) που υποστηρίζει τα πληροφοριακά συστήματα και την επεξεργασία προσωπικών δεδομένων, έτσι ώστε να επιτρέπεται η πρόσβαση μόνο σε εξουσιοδοτημένο προσωπικό (για παράδειγμα, κάποιοι χώροι -όπως αυτοί που βρίσκεται δικτυακός εξοπλισμός- πρέπει να είναι μόνιμα κλειδωμένοι). Σε ορισμένες δε

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

περιπτώσεις (αναλόγως της φύσης των δεδομένων και των υπαρχόντων κινδύνων) ενδέχεται να είναι πρόσφορο να καταγράφεται κάθε πρόσβαση σε συγκεκριμένο φυσικό χώρο.

Β) Τήρηση καταλόγου

Ο υπεύθυνος επεξεργασίας πρέπει να διατηρεί επικαιροποιημένο κατάλογο με τα δικαιώματα φυσικής πρόσβασης του προσωπικού καθώς και με το προσωπικό που διαθέτει κωδικούς, κάρτες εισόδου και κλειδιά για πρόσβαση σε κρίσιμους, ως προς την ασφάλεια, χώρους. Οι κατάλογοι αυτοί θα πρέπει να υπόκεινται σε τακτική αναθεώρηση.

7.7.2. Περιβαλλοντική ασφάλεια

Α) Προστασία από φυσικές καταστροφές

Πρέπει να λαμβάνονται τα κατάλληλα μέτρα για την προστασία των κτιρίων, των κρίσιμων χώρων, του computer room, των γραφείων του προσωπικού, του εξοπλισμού πληροφορικής και του χώρου τήρησης φυσικού αρχείου από ζημιές που μπορούν να προκληθούν από φυσικές καταστροφές ή κακόβουλες ενέργειες, όπως πλημμύρα, υπερθέρμανση, πυρκαγιά, σεισμός, έκρηξη, διαρροή νερού, διακοπή ρεύματος, διάρρηξη/κλοπή, βανδαλισμός, κ.λπ. Ενδεικτικά μέτρα προς αυτή την κατεύθυνση είναι τα εξής: συναγερμός, πόρτες και παράθυρα ασφαλείας, πυροπροστασία, απομάκρυνση εξοπλισμού από υδροσωληνώσεις και πηγές σκόνης, ανιχνευτές υγρασίας και πλημμύρας, αδιάλειπτη παροχή ρεύματος μέσω σταθεροποιητών/γεννητριών, κ.λπ.

7.7.3. Έκθεση εγγράφων

Α) Τοποθέτηση φακέλων

Οι φάκελοι που περιέχουν προσωπικά δεδομένα (φυσικό αρχείο) πρέπει να είναι τοποθετημένοι σε φωριαμούς και να μην εκτίθενται σε κοινή θέα.

Β) Μεταφορά φακέλων

Θα πρέπει να καταγράφεται η μεταφορά των φυσικών φακέλων σε διαφορετικά γραφεία ή οργανωτικές μονάδες.

Γ) Clean desk policy

Δεν θα πρέπει να αφήνονται εκτεθειμένα, χωρίς επίβλεψη, έγγραφα και φορητά μέσα αποθήκευσης πάνω σε γραφεία.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Δ) Συσκευές αναπαραγωγής εγγράφων

Λοιπές συσκευές που δύναται να χρησιμοποιηθούν για υποκλοπή ή για την έκθεση προσωπικών δεδομένων σε κοινή θέα, όπως φωτοαντιγραφικά, συσκευές fax, εκτυπωτές, κ.λπ. θα πρέπει να προστατεύονται κατάλληλα.

7.7.4. Προστασία φορητών μέσων αποθήκευσης

Α) Ασφάλεια φορητών μέσων

Πρέπει να λαμβάνονται τα κατάλληλα μέτρα για τη φυσική ασφάλεια και προστασία των φορητών αποθηκευτικών μέσων - όπως να φυλάσσονται σε ασφαλή σημεία όταν δεν είναι σε χρήση και να είναι πάντα υπό επίβλεψη κατά τη διάρκεια της χρήσης τους.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

8

8. Ασφάλεια κινητών τηλεφώνων (smartphones)

8.1. Εισαγωγή

Τα Smartphones είναι κινητές συσκευές, οι οποίες έχουν τους ίδιους κινδύνους με τους ηλεκτρονικούς υπολογιστές, ωστόσο, διαφέρουν λόγω του μεγέθους τους και τις πιθανές εφαρμογές τους με τους εξής τρόπους:

- Περιβάλλον και χρήση
- Ανάμειξη ιδιωτικής και επαγγελματικής χρήσης
- Χρήση νέων τεχνολογιών
- Μόνιμη σύνδεση στο διαδίκτυο
- Καθορισμός θέσης μέσω GPS, κινητών ραδιοκυττάρων και WLAN
- Ενσωματωμένες κάμερες
- Ευέλικτες επιλογές επικοινωνίας μέσω κυψελοειδούς πρότυπα (UMTS, GSM, LTE), WiFi, Bluetooth, NFC, κτλ.
- Εκτεταμένο λογισμικό
- Συνδυασμός διαφορετικών τεχνολογιών
- Εκλεπτυσμένα λειτουργικά συστήματα
- Ενσωματωμένοι αισθητήρες

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

8.2. Τύποι επίθεσης

Η αρχή είναι μια επίθεση σε έξυπνες υποδομές που βασίζονται τηλέφωνο μια ποικιλία των διαθέσιμων επιλογών. Οι μέθοδοι αυτές κυμαίνονται από την εκμετάλλευση των τρωτών σημείων σε διάφορα εξαρτήματα, για την επίτευξη φυσική πρόσβαση σε ευαίσθητα δεδομένα, στην κοινωνική επιθέσεις που στοχεύουν απευθείας στο προσωπικό ή κοινωνικό περιβάλλον τους.

- Επιθέσεις στο smartphone
    - Στην περίπτωση αυτή, το smartphone είναι το ίδιο το αντικείμενο της επίθεσης, προκειμένου να αποκτήσουν πρόσβαση στα δεδομένα ή το ίδιο το smartphone.

- Επιθέσεις από το smartphone
    - Κατασκοπεία
      Αισθητήρες όπως κάμερες και μικρόφωνα επιτρέψει σε έναν εισβολέα να καταγράφει παράνομα τις συνομιλίες ή φωτογράφηση των κρίσιμων δεδομένων. Λόγω της κινητικότητάς τους έξυπνων τηλεφώνων μπορεί εύκολα να τοποθετηθεί σε κρίσιμα σημεία και προς τα εμπρός καταγεγραμμένα δεδομένα σε τρίτους.

    - Επιθέσεις στο δίκτυο
      Τα Smartphone με κατάλληλο λογισμικό μπορούν να χρησιμοποιηθούν για τη συλλογή δεδομένων σε δίκτυα. Με κακή ασφάλεια ενός ασύρματου δικτύου, το smartphone μπορεί να χρησιμοποιηθεί για περισσότερες πληροφορίες σχετικά με το δίκτυο πίσω από αυτό να συλλέγουν και να χρησιμοποιούν τις πληροφορίες για περαιτέρω επιθέσεις..

8.3. Μέτρα Ασφαλείας για τα κινητά των εργαζομένων σε περίπτωση που συνδέονται με το WiFi της Επιχείρησης.

- Χρησιμοποιήστε έναν ισχυρό κωδικό πρόσβασης για να ασφαλίσετε τις συσκευές των εργαζομένων σας.
- Χρησιμοποιήστε κρυπτογράφηση για την ασφαλή αποθήκευση των δεδομένων στη συσκευή.
- Βεβαιωθείτε ότι η πρόσβαση στη συσκευή είναι κλειδωμένη ή τα δεδομένα να διαγράφονται αυτόματα εάν εισάγεται εσφαλμένος κωδικός πρόσβασης πολλές φορές;
- Βεβαιωθείτε ότι η συσκευή κλειδώνει αυτόματα εάν είναι αδρανής για X χρονικό διάστημα;
- Βεβαιωθείτε ότι οι χρήστες γνωρίζουν ακριβώς ποια δεδομένα μπορούν αυτόματα ή εξ αποστάσεως να διαγραφούν και κάτω από ποιες περιστάσεις.
- Διατηρήστε σαφή διαχωρισμό μεταξύ των προσωπικών δεδομένων που γίνεται επεξεργασία για λογαριασμό του υπεύθυνου επεξεργασίας δεδομένων και του ιδιοκτήτη της συσκευής. Για παράδειγμα, χρησιμοποιώντας διαφορετικές εφαρμογές για επαγγελματική και προσωπική χρήση.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

9

9. Σύνοψη Πολιτικής Ασφάλειας ΠΣ | Οι βασικότερες συμβουλές

Η Πολιτική Ασφάλειας ΠΣ αποτελεί ένα εκτενές κείμενο, το οποίο, αν και είναι γραμμένο σε απλή και απαλλαγμένη από τεχνικούς όρους γλώσσα, δύσκολα θα εντυπωθεί τη μνήμη όσων επιχειρήσουν να το μελετήσουν.

Επιπλέον, πρέπει να ληφθεί υπόψη το γεγονός ότι οι επιμέρους πολιτικές που απαρτίζουν την Πολιτική Ασφάλειας ΠΣ απευθύνονται σε διαφορετικούς αποδέκτες εντός και εκτός της Επιχείρησης. Για παράδειγμα, η Πολιτική Θεμιτών Πρακτικών Χρήσης ΠΣ απευθύνεται στους απλούς χρήστες των συστημάτων, η Πολιτική Διαχείρισης Ασφάλειας ΠΣ στα διοικητικά στελέχη της Επιχείρησης και η Πολιτική Αναδόχων και Συνεργατών απευθύνεται σε άτομα εκτός της Επιχείρησης.

Κατά συνέπεια θα ήταν χρήσιμο να συνταχθούν περιλήψεις των πολιτικών για κάθε κατηγορία αποδεκτών. Οι περιλήψεις θα έχουν τα βασικά σημεία και θα διανέμονται με πρόσφορο τρόπο.

Στις παραγράφους που ακολουθούν προτείνονται τέσσερις περιλήψεις, οι οποίες απευθύνονται στους χρήστες των συστημάτων, στα διοικητικά στελέχη, στους διαχειριστές (μηχανικούς) των συστημάτων και στους εξωτερικούς συνεργάτες, αναδόχους εργασιών και προμηθευτές υπηρεσιών.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

9.1. Σύνοψη Πολιτικής Ασφάλειας ΠΣ για τους χρήστες των συστημάτων

9.1.1. Τι πρέπει να προσέχετε

Η ασφάλεια των Πληροφοριακών Συστημάτων (ΠΣ) της Επιχείρησης αποτελεί ζήτημα μεγάλης σπουδαιότητας. Είναι υποχρέωση όλων των εργαζομένων να συμβάλλουν ενεργά στην προσπάθεια αυτή. Ιδιαίτερη προσοχή οφείλεται στα παρακάτω:

- Η εφαρμογή της Πολιτικής Ασφάλειας ΠΕΣ είναι υποχρεωτική. Όλα τα μέλη του προσωπικού έχουν την υποχρέωση να μελετήσουν τα κείμενα όπου περιγράφεται.
- Η Επιχείρηση θα πραγματοποιεί ελέγχους τήρησης της Πολιτικής Ασφάλειας ΠΣ και διατηρεί το δικαίωμα να επιβάλλει κυρώσεις σε περιπτώσεις παραβίασης.
- Η χρήση των ΠΣ μπορεί να εποπτεύεται από ειδικά εξουσιοδοτημένα για αυτόν το σκοπό άτομα.
- Η Επιχείρηση διατηρεί το δικαίωμα πρόσβασης σε όλα τα δεδομένα που δημιουργούνται και αποθηκεύονται στα ΠΣ της.
- Η Επιχείρηση διατηρεί το δικαίωμα να περιορίσει την πρόσβαση σε συγκεκριμένους Ιστοτόπους (Web Sites) του Παγκόσμιου Ιστού (World Wide Web). Οι χρήστες που χρειάζονται πρόσβαση σε Ιστοτόπους που δεν έχουν εγκριθεί από την Επιχείρηση πρέπει να υποβάλλουν σχετικό αίτημα στον Υπεύθυνο Ασφάλειας ΠΣ.
- Οι χρήστες πρέπει να γνωρίζουν ότι η εμπιστευτικότητα των μηνυμάτων ηλεκτρονικού ταχυδρομείου (emails) και των πληροφοριών που διακινούνται μέσω του Διαδικτύου δεν διασφαλίζεται επαρκώς.

9.1.2. Ασφάλεια Ηλεκτρονικού Υπολογιστή

- Εγκαταστήστε ένα τείχος προστασίας και έλεγχο των ιών στους υπολογιστές σας.
- Βεβαιωθείτε ότι το λειτουργικό σας σύστημα έχει ρυθμιστεί ώστε να λαμβάνει αυτόματες ενημερώσεις.
- Προστατέψτε τον υπολογιστή σας κατεβάζοντας τα πιο πρόσφατα ενημερωμένα ενημερώσεις κώδικα ή ενημερώσεις ασφαλείας, τα οποία πρέπει να καλύπτουν τις ευπάθειες.
- Επιτρέψτε μόνο στο προσωπικό σας πρόσβαση στις πληροφορίες που χρειάζονται για να κάνουν τη δουλειά τους και μην τους αφήνετε να μοιράζονται κωδικούς πρόσβασης.
- Κρυπτογραφήστε τυχόν προσωπικά δεδομένα που κρατούνται ηλεκτρονικά, τα οποία θα μπορούσαν να προκαλέσουν βλάβη ή αγωνία, εάν χάθηκαν ή κλαπηθούν.
- Να λαμβάνετε τακτικά αντίγραφα ασφαλείας των πληροφοριών στο σύστημα του υπολογιστή σας και να τα φυλάτε σε ξεχωριστό μέρος, έτσι ώστε εάν χάσετε τους υπολογιστές σας, δεν χάνετε τις πληροφορίες.
- Αφαιρέστε με ασφάλεια όλες τις προσωπικές πληροφορίες πριν απορρίψετε παλιούς υπολογιστές (χρησιμοποιώντας τεχνολογία ή καταστρέφοντας τον σκληρό δίσκο).
- Εξετάστε την εγκατάσταση ενός εργαλείου προστασίας από spyware. Το λογισμικό υποκλοπής spyware είναι το γενικό όνομα που δίνεται σε προγράμματα που έχουν σχεδιαστεί για την κρυφή παρακολούθηση των δραστηριοτήτων σας στον υπολογιστή σας. Το λογισμικό υποκλοπής spyware μπορεί να εγκατασταθεί άθελά σε άλλες λήψεις αρχείων και προγραμμάτων και η χρήση τους είναι συχνά κακόβουλη. Μπορούν να συλλάβουν κωδικούς πρόσβασης, τραπεζικά διαπιστευτήρια και στοιχεία πιστωτικών καρτών, και στη συνέχεια να τα αναμεταδώσουν σε

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

απατεώνες. Το λογισμικό anti-spyware βοηθά στην παρακολούθηση και προστασία του υπολογιστή σας από τις απειλές κατά του spyware και είναι συχνά ελεύθερη για χρήση και ενημέρωση.

9.1.3. Ασφάλεια ηλεκτρονικού ταχυδρομείου

- Εξετάστε αν το περιεχόμενο του μηνύματος ηλεκτρονικού ταχυδρομείου πρέπει να είναι κρυπτογραφημένο ή προστατευμένο με κωδικό πρόσβασης. Η ομάδα πληροφορικής ή ασφάλειας θα πρέπει να μπορεί να σας βοηθήσει με την κρυπτογράφηση.
- Όταν αρχίζετε να πληκτρολογείτε το όνομα του παραλήπτη, κάποιο λογισμικό ηλεκτρονικού ταχυδρομείου θα προτείνει παρόμοιες διευθύνσεις που έχετε χρησιμοποιήσει πριν. Εάν προηγουμένως έχετε στείλει μηνύματα ηλεκτρονικού ταχυδρομείου σε πολλά άτομα των οποίων το όνομα ή διεύθυνση αρχίζει με τον ίδιο τρόπο - π.χ. "Dave" - η λειτουργία αυτόματης συμπλήρωσης μπορεί να φέρει αρκετούς "Daves". Βεβαιωθείτε ότι έχετε επιλέξει τη σωστή διεύθυνση πριν κάνετε κλικ στο κουμπί αποστολής.
- Εάν θέλετε να στείλετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου σε έναν παραλήπτη χωρίς να αποκαλύψετε τη διεύθυνσή του σε άλλους παραλήπτες, βεβαιωθείτε ότι χρησιμοποιείτε το τυφλό αντίγραφο (bcc), όχι το αντίγραφο άνθρακα (cc). Όταν χρησιμοποιείτε cc, κάθε παραλήπτης του μηνύματος θα μπορεί να δει τη διεύθυνση στην οποία έχει αποσταλεί.
- Προσέξτε όταν χρησιμοποιείτε μια διεύθυνση email ομάδας. Ελέγξτε ποιος είναι στην ομάδα και βεβαιωθείτε ότι πραγματικά θέλετε να στείλετε το μήνυμά σας σε όλους.
- Αν στείλετε ένα ευαίσθητο μήνυμα ηλεκτρονικού ταχυδρομείου από ένα ασφαλές διακομιστή σε έναν επισφαλή παραλήπτη, η ασφάλεια θα απειληθεί. Μπορεί να χρειαστεί να ελέγξετε ότι οι ρυθμίσεις του παραλήπτη είναι αρκετά ασφαλείς πριν να στείλετε το μήνυμά σας.

9.1.4. Ασφάλεια συσκευής φαξ

- Εξετάστε αν η αποστολή των πληροφοριών με άλλο τρόπο εκτός από το φαξ είναι πιο κατάλληλη, όπως η χρήση υπηρεσίας ταχυμεταφορών ή ασφαλούς ηλεκτρονικού ταχυδρομείου. Βεβαιωθείτε ότι στέλνατε μόνο τις απαιτούμενες πληροφορίες. Για παράδειγμα, εάν ένας δικηγόρος σας ζητήσει να προωθήσετε μια δήλωση, στείλτε μόνο τη δήλωση που σας ζητήθηκε, και όχι όλες τις διαθέσιμες πληροφορίες στο αρχείο.
- Βεβαιωθείτε ότι έχετε διπλό έλεγχο του αριθμού φαξ που χρησιμοποιείτε. Είναι καλύτερο να καλέσετε από έναν κατάλογο επαληθευμένων αριθμών.
- Ελέγξτε ότι στέλνετε φαξ στον παραλήπτη με τα κατάλληλα μέτρα ασφαλείας στη θέση του. Για παράδειγμα, το φαξ σας δεν πρέπει να παραμείνει ανεκμετάλλευτο σε γραφείο ανοιχτού σχεδίου.
- Εάν το φαξ είναι ευαίσθητο, ζητήστε από τον παραλήπτη να επιβεβαιώσει ότι είναι στη συσκευή φαξ, είναι έτοιμη να λάβει το έγγραφο και υπάρχει επαρκές χαρτί στο μηχάνημα.
- Κλήση ή αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου για να βεβαιωθείτε ότι το έγγραφο έχει ληφθεί με ασφάλεια.
- Χρησιμοποιήστε ένα φύλλο κάλυψης. Αυτό θα επιτρέψει σε οποιονδήποτε να γνωρίζει ποια είναι η πληροφορία και αν είναι εμπιστευτική ή ευαίσθητη, χωρίς να χρειάζεται να εξετάσει το περιεχόμενο.

9.1.5. Άλλα μέτρα ασφαλείας

- Καταστρέψτε όλα τα απόρρητα απορρίμματα χαρτιού.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

- Ελέγξτε τη φυσική ασφάλεια των χώρων σας.

9.2. Εκπαίδευση και ασφάλεια του προσωπικού

- Εκπαιδεύστε το προσωπικό σας:
  - έτσι ξέρουν τι αναμένεται από αυτούς.
  - να είναι δύσπιστοι απέναντι στους ανθρώπους που μπορεί να προσπαθήσουν να τους εξαπατήσουν να δώσουν προσωπικές λεπτομέρειες.
  - έτσι ώστε να μπορούν να διώκονται εάν σκοπίμως δίνουν προσωπικά στοιχεία χωρίς άδεια.
  - να χρησιμοποιούν έναν ισχυρό κωδικό πρόσβασης.
  - να μην στέλνουν προσβλητικά μηνύματα ηλεκτρονικού ταχυδρομείου σχετικά με άλλους ανθρώπους, την ιδιωτική τους ζωή ή οτιδήποτε άλλο θα μπορούσε να φέρει την οργάνωση σας σε ατιμία.
  - να μην πιστεύουν ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου που προέρχονται από την τράπεζά σας ζητούν τον λογαριασμό σας, τα στοιχεία πιστωτικών καρτών ή τον κωδικό πρόσβασής σας (μια τράπεζα δεν θα ζητούσε ποτέ αυτές τις πληροφορίες με αυτόν τον τρόπο).
  - να μην ανοίξετε το spam - ούτε καν να διαγραφείτε ή να ζητήσετε περισσότερες αποστολές μηνυμάτων. Πείτε τους να διαγράψουν το ηλεκτρονικό ταχυδρομείο και είτε να πάρουν φίλτρα ανεπιθύμητης αλληλογραφίας στους υπολογιστές σας είτε να χρησιμοποιήσουν έναν παροχέα email που προσφέρει αυτή την υπηρεσία.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

I

10. Παράρτημα Ι – Διαδικασία τήρησης εφεδρικών αντιγράφων ασφαλείας

10.1. Εισαγωγή

Η τήρηση εφεδρικών αντιγράφων (Backup) μας βοηθά να προστατεύουμε τα σημαντικά δεδομένα που έχουμε στον Ηλεκτρονικού Υπολογιστή μας. Τα δεδομένα αυτά διατρέχουν κίνδυνο να καταστραφούν (μερικώς ή ολικώς) από:

- Ανθρώπινο λάθος.
- Καταστροφή ή δυσλειτουργία του λογισμικού.
- Καταστροφή ή δυσλειτουργία του υλικού.
- Ιούς.
- Κλοπή και λοιπές καταστροφές.

10.2. Τήρηση αντιγράφων ασφαλείας

Ο υπεύθυνος πληροφορικής πρέπει να αναπτύξει συγκεκριμένη πολιτική για τη λήψη και διαχείριση των αντιγράφων ασφαλείας. Η πολιτική πρέπει να περιλαμβάνει τουλάχιστον τους κανόνες/διαδικασίες που αφορούν τα εξής: την επιλογή των κρίσιμων πόρων (εφαρμογές, λειτουργικά συστήματα, αρχεία, δεδομένα αρχείων χρηστών, κ.λπ.) που χρήζουν δημιουργίας αντιγράφων ασφαλείας, τη συχνότητα της δημιουργίας/λήψης των αντιγράφων ασφαλείας (ανά τακτά διαστήματα, σε ημερήσια ή εβδομαδιαία βάση, ανάλογα με το μέγεθος και το είδος των δεδομένων, καθώς και με το πότε αυτά μεταβάλλονται), την

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

κατάλληλη επισήμανση αυτών, την ασφαλή αποθήκευσή τους και την ορθή ανάκτηση των δεδομένων από τα αντίγραφα ασφαλείας (συμπεριλαμβανομένου του περιοδικού ελέγχου ακεραιότητας/αξιοπιστίας των αντιγράφων που λαμβάνονται). Τα παραπάνω πρέπει να εξασφαλίζουν ότι σε περίπτωση εκτάκτων περιστατικών ασφαλείας και απώλειας ή καταστροφής δεδομένων για άλλη αιτία (π.χ. αστοχία υλικού), η διαθεσιμότητα και ακεραιότητα αυτών παραμένει.

10.3. Τόπος τήρησης

Κάποιο αντίγραφο ασφαλείας πρέπει να διατηρείται σε διαφορετικό χώρο/φυσική τοποθεσία από τα πρωτογενή δεδομένα, ο οποίος να διαθέτει μέτρα ασφαλείας ανάλογα με τα μέτρα που υιοθετούνται για τα πρωτογενή δεδομένα. Επίσης, να λαμβάνονται μέτρα για την ασφαλή μεταφορά του.

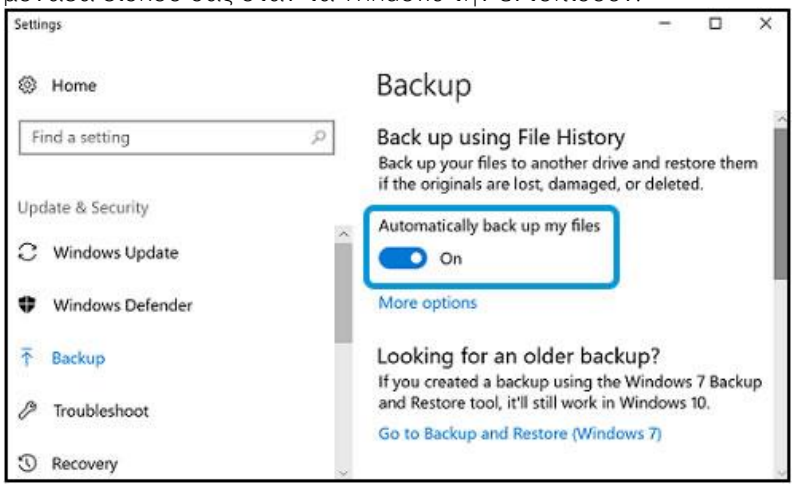
10.4. Βήματα για τη δημιουργία αντιγράφων ασφαλείας στα Windows 10

1. Συνδέστε την εξωτερική μονάδα δίσκου με τον υπολογιστή. Αν ανοίξει ένα παράθυρο αυτόματης εκτέλεσης, κλείστε το.

2. Χρησιμοποιήστε το πλαίσιο αναζήτησης στη γραμμή εργασιών για να βρείτε και να ανοίξετε τις Ρυθμίσεις αντιγράφων ασφαλείας.

3. Ενεργοποίηση του στοιχείου Αυτόματη δημιουργία αντιγράφων ασφαλείας των αρχείων μου.

   Σημείωση: Αν δεν εμφανίζεται η επιλογή Αυτόματη δημιουργία αντιγράφων ασφαλείας των αρχείων μου, επιλέξτε Προσθήκη μονάδας δίσκου και, στη συνέχεια, επιλέξτε την εξωτερική μονάδα δίσκου σας όταν τα Windows την εντοπίσουν.

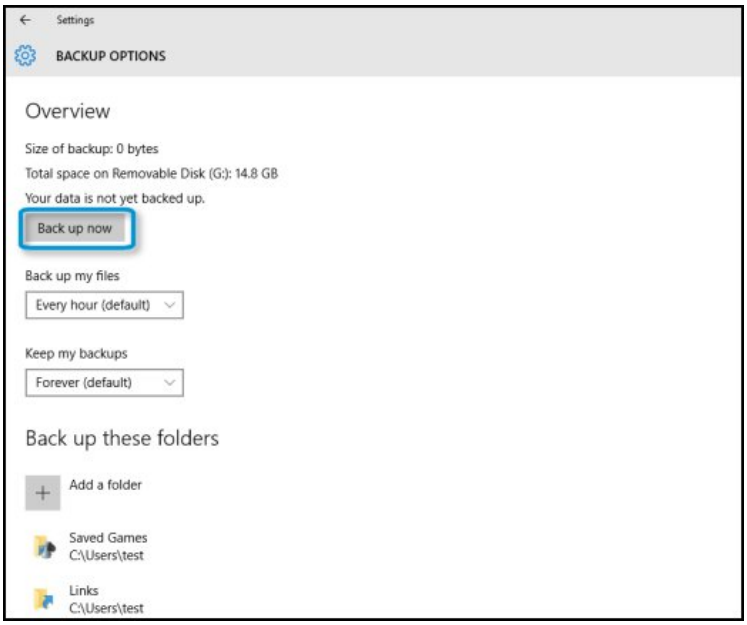


Εικόνα: Ενεργοποίηση της αυτόματης δημιουργίας αντιγράφων ασφαλείας

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

4. Για να δημιουργήσετε άμεσα αντίγραφα ασφαλείας των αρχείων σας ή για να προσαρμόσετε τις ρυθμίσεις της δημιουργίας αντιγράφων ασφαλείας, επιλέξτε το στοιχείο Περισσότερες επιλογές.

   - Για να δημιουργήσετε άμεσα αντίγραφα ασφαλείας των αρχείων σας, επιλέξτε Άμεση δημιουργία αντιγράφων ασφαλείας.



Εικόνα: Επιλογή του στοιχείου Άμεση δημιουργία αντιγράφων ασφαλείας

   - Για να εξαιρέσετε συγκεκριμένους φακέλους από τα αντίγραφα ασφαλείας, προσθέστε τους στην περιοχή Εξαίρεση αυτών των φακέλων.

Εικόνα: Περιοχή Εξαίρεση αυτών των φακέλων

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

- Για να ρυθμίσετε τη συχνότητα αυτόματης δημιουργίας αντιγράφων ασφαλείας των αρχείων σας από τα Windows, κάντε μια επιλογή στο αναπτυσσόμενο μενού Δημιουργία αντιγράφων ασφαλείας των αρχείων μου.

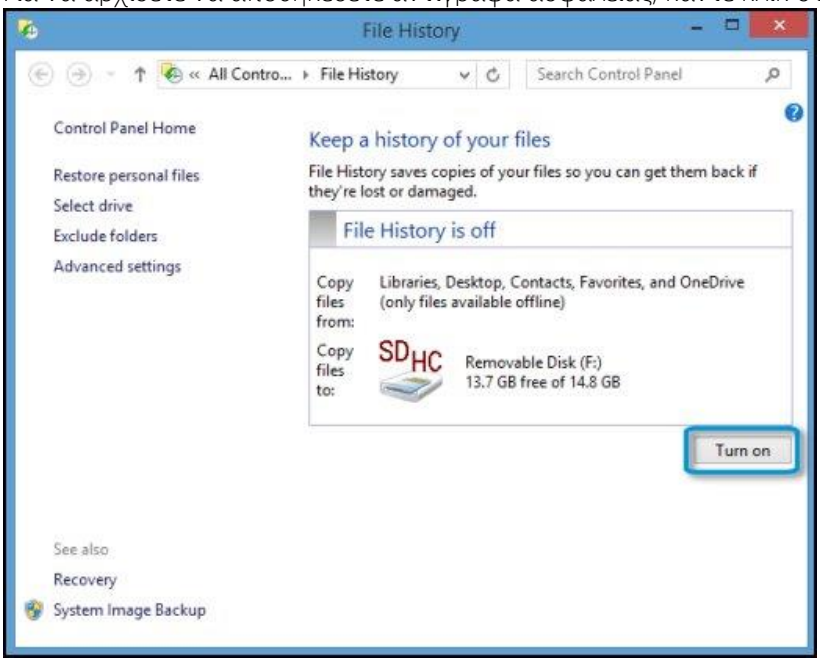
- Για να ορίσετε το διάστημα που επιθυμείτε τα Windows να διατηρήσουν τα αρχεία σας, κάντε μια επιλογή στο αναπτυσσόμενο μενού Διατήρηση των αντιγράφων ασφαλείας μου.

10.5. Βήματα για τη δημιουργία αντιγράφων ασφαλείας στα Windows 8

1. Συνδέστε την εξωτερική μονάδα δίσκου με τον υπολογιστή. Αν ανοίξει ένα παράθυρο αυτόματης εκτέλεσης, κλείστε το.

2. Στα Windows, κάντε αναζήτηση για το στοιχείο Αποθήκευση των αντιγράφων ασφαλείας και ανοίξτε το.

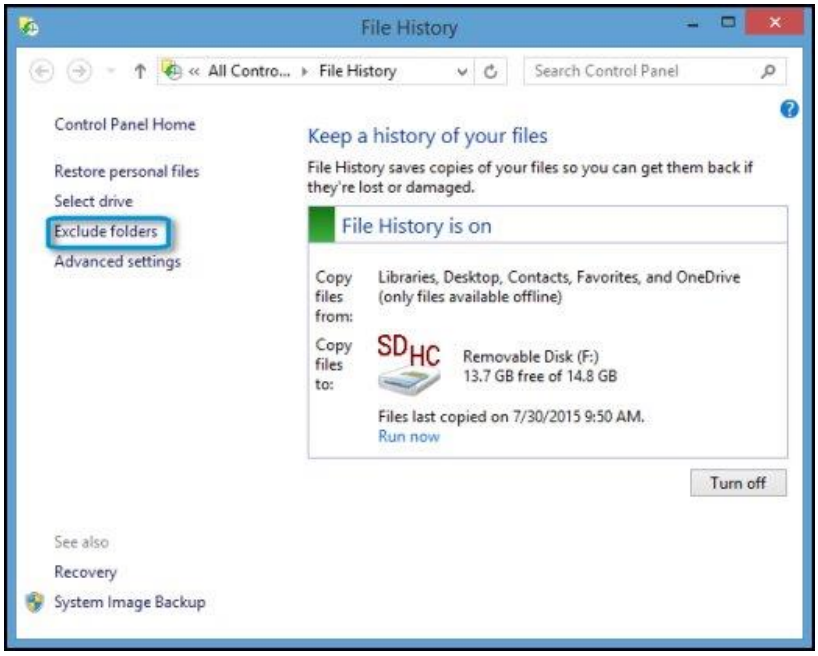
3. Για να αρχίσετε να αποθηκεύετε αντίγραφα ασφαλείας, κάντε κλικ στο Ενεργοποίηση.



Εικόνα: Ενεργοποίηση του Ιστορικού αρχείων

4. Αν υπάρχουν συγκεκριμένοι φάκελοι ή βιβλιοθήκες για τα οποία δεν επιθυμείτε να δημιουργηθούν αντίγραφα ασφαλείας, επιλέξτε Εξαίρεση φακέλων και, στη συνέχεια, προσθέστε τα στοιχεία στις βιβλιοθήκες φακέλων που εξαιρούνται.

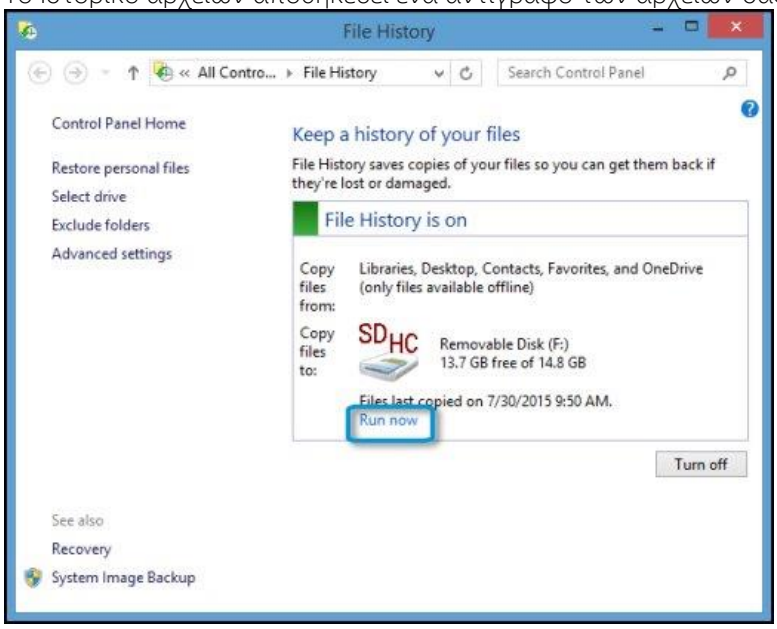
Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr



Εικόνα: Εξαίρεση φακέλων

5. Για να δημιουργήσετε άμεσα αντίγραφα ασφαλείας των αρχείων σας, κάντε κλικ στο Άμεση εκτέλεση.

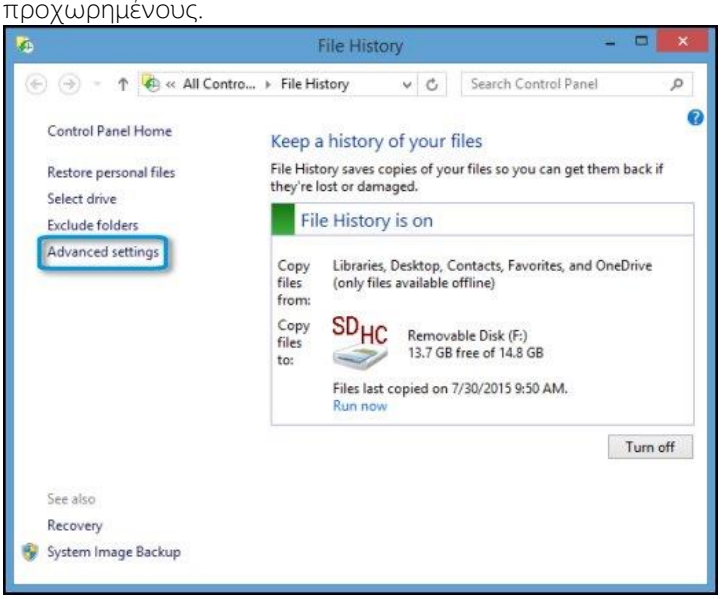
6. Το Ιστορικό αρχείων αποθηκεύει ένα αντίγραφο των αρχείων σας.



Εικόνα: Επιλογή του στοιχείου Άμεση εκτέλεση

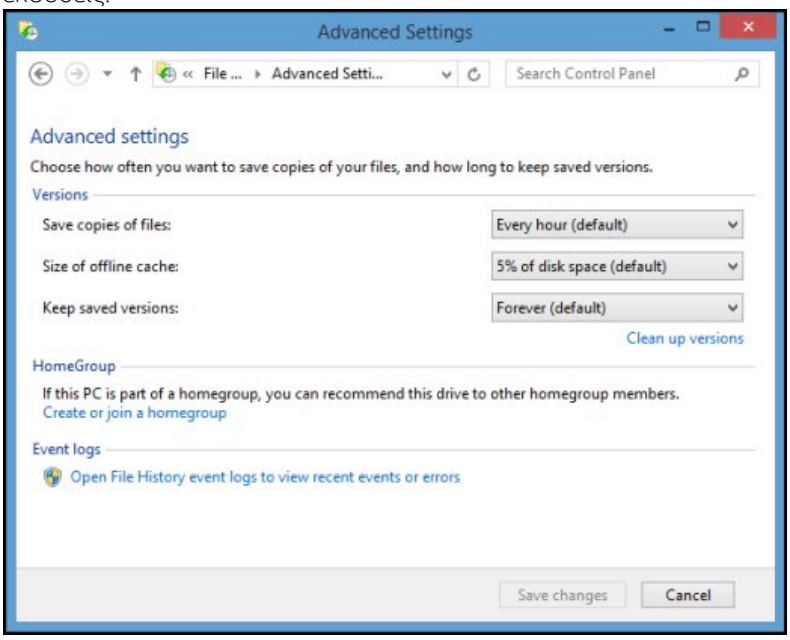
Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

7. Για να προσαρμόσετε τις ρυθμίσεις δημιουργίας αντιγράφων ασφαλείας, επιλέξτε Ρυθμίσεις για προχωρημένους.



Εικόνα: Κλικ στην επιλογή Ρυθμίσεις για προχωρημένους

8. Στις Ρυθμίσεις για προχωρημένους επιλέξτε πόσο συχνά θέλετε να αποθηκεύονται αντίγραφα ασφαλείας των αρχείων σας και για πόσο διάστημα θέλετε να διατηρούνται οι αποθηκευμένες εκδόσεις.



Εικόνα: Παράθυρο "Ρυθμίσεις για προχωρημένους"

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

10.6. Επαναφορά αποθηκευμένων αρχείων με το ιστορικό αρχείων

Με το Ιστορικό αρχείων μπορείτε να επαναφέρετε ένα ή όλα τα αρχεία που έχετε αποθηκεύσει σε αντίγραφα ασφαλείας. Επίσης, μπορείτε να βρείτε διαφορετικές εκδοχές των αρχείων σας από συγκεκριμένες ημερομηνίες.

1. Συνδέστε την εξωτερική μονάδα δίσκου με τον υπολογιστή. Αν ανοίξει ένα παράθυρο αυτόματης εκτέλεσης, κλείστε το.

2. Στα Windows, πραγματοποιήστε αναζήτηση για το στοιχείο Επαναφορά των αρχείων σας με το Ιστορικό αρχείων και ανοίξτε το.

3. Κάντε κλικ στα εικονίδια Προηγούμενο και Επόμενο για να επιλέξετε το σημείο δημιουργίας αντιγράφων ασφαλείας που θέλετε να επαναφέρετε.

Εικόνα: Εικονίδια Προηγούμενο και Επόμενο

4. Επιλέξτε τα αρχεία ή φακέλους για επαναφορά.

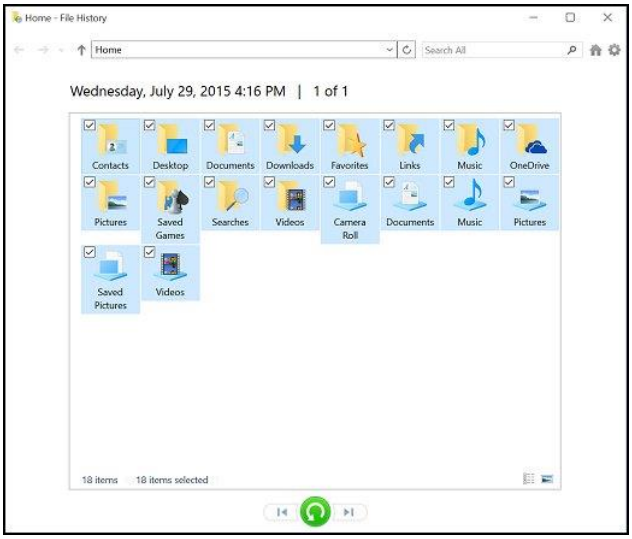
   - Για να επιλέξετε ένα φάκελο: Κάντε κλικ στο φάκελο.

   - Για να επιλέξετε ορισμένους από τους φακέλους: Κρατήστε πατημένο το πλήκτρο ctrl ενώ επιλέγετε τους φακέλους.

   - Για να επιλέξετε όλους τους φακέλους: Κάντε δεξί κλικ σε μια ελεύθερη περιοχή στο παράθυρο της εφαρμογής και, στη συνέχεια, επιλέξτε Επιλογή όλων.

   - Για να επιλέξετε ένα ή περισσότερα αρχεία σε ένα φάκελο: Κάντε διπλό κλικ στο φάκελο και, στη συνέχεια, επιλέξτε τα επιθυμητά αρχεία.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr



Εικόνα: Επιλογή όλων των φακέλων

5. Κάντε κλικ στο εικονίδιο Επαναφορά.

    - Τα Windows επαναφέρουν τα αρχεία.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

11. Παράρτημα II – Ενημέρωση λειτουργικού συστήματος (Windows Updates)

Η ενημέρωση του λειτουργικού συστήματος μπορεί να πραγματοποιείται αυτόματα μέσω του Windows Update. Το Windows Update ελέγχει το λειτουργικό του Η/Υ, καθώς και οποιοδήποτε άλλο λογισμικό της Microsoft, και φροντίζει για την απόκτηση όλων των τελευταίων εκδόσεων και κρίσιμων αναβαθμίσεων που χρειάζονται.

11.1.Αυτόματη Ενημέρωση (Automatic Updates)

Επιλέξτε Start (Έναρξη) -> Control Panel -> Windows Update ή Automatic Updates, ή μπορείτε να επισκεφτείτε το διαδικτυακό τόπο της Microsoft μέσω του φυλλομετρητή Internet Explorer (http://windowsupdate.microsoft.com) και να επιλέξετε την οδηγία Turn On Automatic Updates (βρίσκεται στα δεξιά της οθόνης). Ακολούθως καθορίστε την ημέρα και την ώρα που θέλετε να γίνεται η ενημέρωση του λειτουργικού συστήματος. Σε περίπτωση που είναι ήδη ενεργοποιημένη, αναγράφεται ότι είναι "Turn On" και μπορείτε να ελέγξετε/αλλάξετε το χρόνο αυτόματης ενημέρωσης, αν το επιθυμείτε.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

11.2. Μη Αυτόματη Ενημέρωση (Manual Update)

Επιλέξτε Start (Έναρξη) -> Windows Update ή επισκεφτείτε το διαδικτυακό τόπο της Microsoft (http://windowsupdate.microsoft.com) και ακολουθήστε τις σχετικές οδηγίες ως ακολούθως:

Επιλέξτε Express. Θα ακολουθήσει έλεγχος του Η/Υ και όταν ολοκληρωθεί θα εμφανιστούν οι ενημερώσεις που θα γίνουν.

Επιλέξτε Install Updates.

ii

Σε περίπτωση που η ενημέρωση του λειτουργικού συστήματος δεν είναι αυτόματη, θα πρέπει η προαναφερθείσα διαδικασία να γίνεται τουλάχιστο μία φορά την εβδομάδα.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

12. Παράρτημα III – Ιοί Ηλεκτρονικών Υπολογιστών

Ο ιός Η/Υ είναι ένα κακόβουλο λογισμικό που εξαπλώνεται από έναν Η/Υ σε έναν άλλο και παρεμβαίνει στη λειτουργία του. Ένας ιός μπορεί να καταστρέψει ή να διαγράψει δεδομένα σε έναν Η/Υ, να χρησιμοποιήσει ένα πρόγραμμα ηλεκτρονικού ταχυδρομείου για να μεταδώσει τον εαυτό του σε άλλους υπολογιστές ή ακόμα και να διαγράψει όλα τα αρχεία από το σκληρό δίσκο.

Οι ιοί υπολογιστών μεταδίδονται πιο εύκολα από αρχεία/έγγραφα που επισυνάπτονται σε μηνύματα ηλεκτρονικού ταχυδρομείου ή μέσω άμεσων μηνυμάτων. Επομένως, ο χρήστης δεν πρέπει να ανοίγει ποτέ ένα συνημμένο αρχείο/έγγραφο ηλεκτρονικού ταχυδρομείου εκτός και αν γνωρίζει τον αποστολέα του μηνύματος, ή/και αναμένει το συνημμένο αρχείο/έγγραφο. Οι ιοί υπολογιστών μπορεί να εμφανίζονται ως συνημμένες αστείες εικόνες, ευχετήριες κάρτες ή αρχεία ήχου ή βίντεο, ή να κρύβονται σε πειρατικό λογισμικό ή σε άλλα αρχεία ή προγράμματα που μπορεί να μεταφορτώνονται (download) από το διαδίκτυο.

Επίσης, οι ιοί μεταδίδονται πολύ εύκολα με την ανεξέλεγκτη χρήση των memory sticks (USBs), γι' αυτό και οι χρήστες πρέπει να είναι πολύ προσεκτικοί και να ελέγχουν τα USBs με το πρόγραμμα προστασίας από ιούς (antivirus).

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

12.1. Συμπτώματα Ηλεκτρονικού Υπολογιστή σε περίπτωση μόλυνσης από ιό (Virus)

- Ο Η/Υ λειτουργεί πιο αργά από ότι συνήθως.
- Η λειτουργία του Η/Υ σταματάει ή κλειδώνει συχνά.
- Ο Η/Υ παρουσιάζει σφάλματα και μετά κάνει επανεκκίνηση κάθε λίγα λεπτά.
- Ο Η/Υ επανεκκινεί μόνος του.
- Οι εφαρμογές στον Η/Υ δεν λειτουργούν σωστά.
- Δεν είναι δυνατή η πρόσβαση στους δίσκους ή στις μονάδες δίσκου.
- Δεν είναι δυνατή η σωστή εκτύπωση.
- Εμφανίζονται ασυνήθιστα μηνύματα σφάλματος.
- Εμφανίζονται παραμορφωμένα μενού και παράθυρα διαλόγου.
- Υπάρχει διπλή επέκταση σε ένα συνημμένο αρχείο/έγγραφο που ανοίξατε πρόσφατα (π.χ. .jpg.vbs, .gif.exe.).
- Το πρόγραμμα προστασίας από ιούς απενεργοποιήθηκε χωρίς λόγο. Επιπλέον, δεν είναι δυνατή η επανεκκίνηση του προγράμματος προστασίας από ιούς.
- Δεν μπορεί να εγκατασταθεί ένα πρόγραμμα προστασίας από ιούς στον Η/Υ ή το πρόγραμμα προστασίας από ιούς δεν εκτελείται.
- Εμφανίζονται νέα εικονίδια στην επιφάνεια εργασίας, τα οποία δεν τοποθετήθηκαν από το χρήστη ή δε σχετίζονται με κανένα από τα προγράμματα που εγκαταστάθηκαν πρόσφατα.
- Παρατηρείται απροσδόκητη αναπαραγωγή περίεργων ήχων ή μουσικής από τα ηχεία.
- Κάποιο πρόγραμμα εξαφανίζεται από τον Η/Υ, παρόλο που έχει διαγραφεί από το χρήστη.

Σημ.: Αυτές είναι οι συνηθισμένες ενδείξεις μόλυνσης. Ωστόσο, αυτές οι ενδείξεις μπορεί επίσης να προκληθούν από προβλήματα υλισμικού ή λογισμικού που δεν έχουν σχέση με ιούς υπολογιστών.

12.2. Είδη Ιών

- Trojan horses/Backdoor programs: η πιο διαδεδομένη κατηγορία ιών. Αυτού του είδους ιοί συνήθως διαγράφουν αρχεία από τον Η/Υ ή και σε κάποιες περιπτώσεις φορμάρουν το σκληρό δίσκο! Οι Trojan horses δεν αναπαράγονται γι' αυτό και δε θεωρούνται από πολλούς ως ιοί.
- Πολυμορφικοί: οι ιοί που κρύβουν τον κώδικά τους με διαφορετικό τρόπο, κάθε φορά που μολύνουν ένα αρχείο (συνήθως .exe, .com). Έτσι, όταν ο χρήστης εκτελέσει το μολυσμένο αρχείο, ο ιός «ξεκλειδώνει» τον καταστροφικό κώδικα μέσα από το μολυσμένο αρχείο και τον εκτελεί. Αυτός ο τύπος ιών αποτελεί ένα ιδιαίτερο «πονοκέφαλο» για τα προγράμματα antivirus, διότι δεν υπάρχει πάντα ένα συγκεκριμένο/παρόμοιο κομμάτι του ιού για να χρησιμοποιηθεί για την αναγνώρισή του.
- Worms (σκουλήκια): λέγονται έτσι γιατί συνήθως βρίσκονται σε δίκτυα Η/Υ. Χρησιμοποιούν το τοπικό δίκτυο ή/και το διαδίκτυο ως μέσο διάδοσής τους.
- Stealth Viruses (αόρατοι ιοί): χρησιμοποιούν τους καταχωρητές (Registers) του Η/Υ και είναι ικανοί να κρύβονται κατά την ανίχνευσή τους από τα προγράμματα antivirus. Συγκεκριμένα, όποτε εντοπίζουν δράση προγράμματος antivirus, αποκαθιστούν προσωρινά το αρχικό αρχείο, αφήνοντας το antivirus να το ανιχνεύσει και το ξανά-μολύνουν αργότερα, αφού έχει τελειώσει η

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

λειτουργία του προγράμματος antivirus. Η συγκεκριμένη λειτουργία της απόκρυψης του ιού από το antivirus (αντιantivirus) λέγεται και "tunneling".

- Parasitic Appending Viruses: λέγονται παρασιτικοί ή και επι-προσθετικοί ιοί, ακριβώς γιατί προσθέτουν τον καταστροφικό τους κώδικα μέσα στον κώδικα του αρχείου/προγράμματος (συνήθως στο τέλος του, για προστασία από ανίχνευση antivirus προγράμματος), χωρίς να το καταστρέψουν. Κατά την εκτέλεση του προγράμματος, ο ιός φροντίζει να εκτελείται αυτός και όχι το αρχικό πρόγραμμα.
- Overwriting Viruses: ο απλούστερος τρόπος για να μολύνεις ένα σύστημα είναι να αντικαταστήσεις το αρχικό αρχείο με τον ιό. Με τον τρόπο αυτό δεν υπάρχει δυνατότητα αποκατάστασης (καθαρισμού) του αρχικού αρχείου. Οι ιοί αυτοί μπορούν ακόμα να διατηρούν το αρχικό μέγεθος του αρχείου, αποφεύγοντας έτσι την ανίχνευσή τους από προγράμματα antivirus.
- Companion Viruses: ενεργούν κυρίως σε λειτουργικό σύστημα MS-DOS. Αν ο χρήστης θελήσει να εκτελέσει μια εντολή DOS π.χ. Program1.exe, ενώ ταυτόχρονα υπάρχει στο δίσκο και ο ιός με το όνομα Program1.com, τότε με την πληκτρολόγηση μόνον του ονόματος της εντολής "Program1" χωρίς το ".exe" θα εκτελεστεί πρώτα το αρχείο που περιέχει τον ιό (Program1.com).
- Retro Viruses: στοχεύουν αποκλειστικά στην καταπολέμηση ενός ή περισσοτέρων προγραμμάτων antivirus.
- Logic Bombs: πρόκειται για ιούς που ενεργοποιούνται όταν επέλθει μια συγκεκριμένη χρονική στιγμή, π.χ. στις 13 του Σεπτέμβρη, ώρα 14:00. Συνήθως επιτελούν καταστροφικό έργο, όπως η διαγραφή αρχείων.
- Droppers: είναι εκτελέσιμα αρχεία (executables) που περιέχουν εντολές για τη δημιουργία ιού μέσα στο σύστημα και δεν περιέχουν τον ίδιο τον ιό. Ανιχνεύονται πιο δύσκολα σε σύγκριση με άλλους ιούς.
- Boot Sector Viruses: οι ιοί αυτού του είδους μολύνουν τον τομέα εκκίνησης του Η/Υ. Σε αυτούς οφείλεται το μεγαλύτερο ποσοστό μολύνσεων ανά τον κόσμο.
- Direct Action Viruses: οι εν λόγω ιοί εκτελούν το καταστροφικό τους έργο μια φορά μόνο, όταν ενεργοποιηθούν και δεν μένουν στην μνήμη του Η/Υ.
- Macro Viruses: μολύνουν μόνο έγγραφα τύπου Word, Excel, Office, PowerPoint, Access, χρησιμοποιώντας μια μακρό-εντολή.
- Multi Platform Viruses: επιδρούν σε περισσότερα από ένα λειτουργικά συστήματα.

12.3. Τρόποι Προστασίας από Ιούς

- Να τηρούνται εφεδρικά αντίγραφα ασφάλειας σε CD ή USB ή εξωτερικό δίσκο.
- Να γίνεται τακτική ανίχνευση του δίσκου με το πρόγραμμα προστασίας, η βάση δεδομένων του οποίου πρέπει να ενημερώνεται/επικεροποιείται (update) καθημερινά.
- Να γίνεται ανίχνευση κάθε νέου αρχείου που «μεταφορτώνεται» από το διαδίκτυο.
- Να μη γίνεται εισαγωγή USB στον Η/Υ από άτομα που δε γνωρίζει ο χρήστης. Να γίνεται έλεγχος του USB με το πρόγραμμα προστασίας από ιούς (antivirus) πριν να χρησιμοποιηθεί.
- Να γίνει απενεργοποίηση της αυτόματης εκτέλεσης των CD/USB στον Η/Υ.
- Να γίνει επιλογή της πλήρης εμφάνισης των τύπων αρχείων στον Η/Υ.

Σημ.: Στις περιπτώσεις όπου δεν υπάρχουν εγκατεστημένα προγράμματα προστασίας από ιούς στους Η/Υ, οι χρήστες θα πρέπει να επικοινωνούν άμεσα με τη Διοίκηση.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

IV

13. Παράρτημα IV – Ιστορικό Περιήγησης (History) – Μπισκοτάκια (Cookies) – Προσωρινή Μνήμη (Cashe Memory)

Όλοι οι φυλλομετρητές (browsers) τηρούν Ιστορικό (History) όλων των ιστοσελίδων που έχει επισκεφτεί ο χρήστης. Ο χρήστης μπορεί να διαγράψει αυτές τις πληροφορίες για σκοπούς προστασίας της Ιδιωτικότητας του (Privacy), αλλά και για σκοπούς εξυπηρέτησης χώρου στο σκληρό δίσκο.

Τα Μπισκοτάκια δεδομένων (Cookies) είναι μικρά "αρχεία" που περιέχουν πληροφορίες τις οποίες χρησιμοποιούν οι ιστοσελίδες για την αναγνώρισή του Η/Υ του χρήστη.

Η Προσωρινή Μνήμη (Cache Memory) είναι ένας συγκεκριμένο χώρος στον Η/Υ στον οποίο αποθηκεύονται προσωρινά κάποια στοιχεία. Όταν ο χρήστης ανοίξει μια ιστοσελίδα, ο φυλλομετρητής αποθηκεύει προσωρινά κάποια στοιχεία σε αυτό το χώρο. Όταν κλείσει ο φυλλομετρητής, τα αρχεία αυτά δε διαγράφονται αλλά παραμένουν στον Η/Υ για μελλοντική χρήση. Η προσωρινή μνήμη επιταχύνει τη λειτουργία του Η/Υ αφού ο φυλλομετρητής ελέγχει αν ο χρήστης έχει επισκεφθεί ήδη την ιστοσελίδα και αν έχει αλλάξει κάτι από την προηγούμενη φορά. Αν δεν έχει αλλάξει οτιδήποτε, η ιστοσελίδα φορτώνεται από την προσωρινή μνήμη χωρίς να χρειάζεται να καταφορτωθεί ξανά από το διαδίκτυο.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Όμως, με την πάροδο του χρόνου, η προσωρινή μνήμη αρχίζει να καταλαμβάνει περισσότερο χώρο με αρχεία τα οποία πολλές φορές δε θα χρειαστούν ξανά.

Επίσης, πολλές φορές η προσωρινή μνήμη μπορεί να δημιουργήσει προβλήματα στην περιήγηση, αφού μπορεί να εμφανίζει παλαιότερο περιεχόμενο και πολύ πιθανό λανθασμένο. Είναι χρήσιμο λοιπόν να διαγράφεται τακτικά το περιεχόμενο της προσωρινής μνήμης του Η/Υ.

Διαγραφή Ιστορικού Περιήγησης – Cookies – Προσωρινής Μνήμης

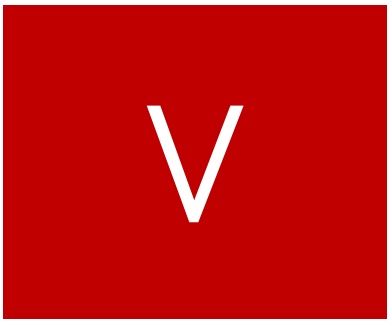
Η διαγραφή του Ιστορικού Περιήγησης, των Cookies και της Προσωρινής Μνήμης γίνεται με διαφορετικό τρόπο, ανάλογα με το φυλλομετρητή που χρησιμοποιεί ο χρήστης. Για παράδειγμα:

Internet Explorer 8
Επιλέξτε **Εργαλεία (Tools)** -> Επιλογές **Διαδίκτυο (Internet Options)** -> **Γενικά (General)**. Στο τμήμα **Browsing History** επιλέξτε την οδηγία **Delete**. Τότε εμφανίζεται ένα παράθυρο όπου είναι επιλεγμένα με √ τα αρχεία που θα διαγραφούν (συνήθως είναι επιλεγμένα τα Temporary Internet Files (Cache), Cookies, History και Pre-serve Favorites Website Data). Από το παράθυρο αυτό επιλέξτε την οδηγία **Delete**. Αν κάποια αρχεία δεν επιθυμείτε να διαγραφούν τότε απενεργοποιήστε τα, κάνοντας κλικ στο κουτάκι που υπάρχει √, ώστε να αφαιρεθεί το √ και συνεπώς να μην συμπεριληφθούν τα συγκεκριμένα αρχεία στη διαδικασία διαγραφής.

Mozilla Firefox 7.0.1
Επιλέξτε **Εργαλεία (Tools)** -> Επιλογές **(Options)** -> Προσωπικά **(Privacy)**.
Επιλέξτε την οδηγία **Clear your recent History**. Τότε εμφανίζεται ένα παράθυρο όπου είναι επιλεγμένα με √τα αρχεία που θα διαγραφούν (συνήθως είναι επιλεγμένα τα Cache, Cookies, Active Logins). Από το παράθυρο αυτό επιλέξτε την οδηγία **Clear Now**. Αν κάποια αρχεία δεν επιθυμείτε να διαγραφούν τότε απενεργοποιήστε τα, κάνοντας κλικ στο κουτάκι που υπάρχει √, ώστε να αφαιρεθεί το √ και συνεπώς να μην συμπεριληφθούν τα συγκεκριμένα αρχεία στη διαδικασία διαγραφής.

Σημ.: *Οδηγίες για άλλες εκδόσεις των υπό αναφορά φυλλομετρητών ή για άλλους φυλλομέτρητες μπορείτε να επικοινωνήστε με τον Υπεύθυνο Πληροφοριακών Συστημάτων.*

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr



14. Παράρτημα V – Ανεπιθύμητες ηλεκτρονικές επικοινωνίες | SPAM

Η αζήτητη ηλεκτρονική επικοινωνία, δηλαδή κάθε ηλεκτρονικό μήνυμα που αποστέλλεται με σκοπό, την εμπορική προώθηση προϊόντων ή υπηρεσιών ή και κάθε άλλο διαφημιστικό σκοπό χωρίς ο παραλήπτης να έχει δώσει τη συγκατάθεσή του για αυτό, αναφέρεται διεθνώς με τον όρο "spam". Τα μηνύματα spam μπορεί να αποσκοπούν σε οποιονδήποτε διαφημιστικό σκοπό, π.χ. να προωθούν δράσεις φιλανθρωπικών ιδρυμάτων ή πολιτικών κομμάτων. Η πρακτική του "spamming" μπορεί να απαντηθεί σε πολλές περιπτώσεις ηλεκτρονικής επικοινωνίας, όπως:

- σε μηνύματα ηλεκτρονικού ταχυδρομείου
- στις υπηρεσίες μηνυμάτων με χρήση κινητής τηλεφωνίας (SMS, MMS)
- στις υπηρεσίες φαξ
- στις υπηρεσίες στιγμιαίων μηνυμάτων (instant messaging), π.χ. MSN, Yahoo Messenger, Google Chat, κ.ά.
- στις υπηρεσίες ηλεκτρονικής ανταλλαγής μηνυμάτων, όπως σελίδες κοινωνικής δικτύωσης, π.χ. Facebook, Twitter, Myspace κ.ά.

Οι αποστολείς μηνυμάτων spam είναι γνωστοί και ως spammers.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

Σε όλη την Ευρωπαϊκή Ένωση, για την αποστολή διαφημίσεων με αυτοματοποιημένα μέσα, ισχύει το λεγόμενο σύστημα «opt-in», δηλαδή η αποστολή τους επιτρέπεται μόνον κατόπιν ρητής συγκατάθεσης του παραλήπτη, με ελάχιστες εξαιρέσεις. Στα μέσα αυτά, με τα οποία η επικοινωνία πραγματοποιείται χωρίς ανθρώπινη παρέμβαση, συμπεριλαμβάνονται τα μηνύματα ηλεκτρονικού ταχυδρομείου στο διαδίκτυο, τα μηνύματα σε δίκτυα κινητής τηλεφωνίας (SMS, MMS), τα φαξ κ.λπ. Εξαίρεση στον κανόνα αυτόν αποτελεί η περίπτωση στην οποία τα στοιχεία επικοινωνίας του παραλήπτη αποκτήθηκαν από τον αποστολέα στο πλαίσιο παρόμοιας, προηγούμενης συναλλαγής, κυρίως πώλησης παρόμοιων προϊόντων ή υπηρεσιών. Επιπλέον, σε κάθε μήνυμα, ακόμα και σε αυτά που στέλνονται με συγκατάθεση, πρέπει να αναγράφεται η ταυτότητα του αποστολέα και να παρέχεται ένας έγκυρος τρόπος τερματισμού της περαιτέρω αποστολής τέτοιων μηνυμάτων.

Ειδικότερα, στο άρθρο 11 του ν. 3471/2006, ο οποίος μεταφέρει στην ελληνική νομοθεσία την αντίστοιχη διάταξη του άρθρου 13 της Οδηγίας 2002/58/ΕΚ ορίζονται τα εξής: «Η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς».

Με άλλα λόγια, κάθε ηλεκτρονικό μήνυμα που αποστέλλεται χωρίς την προηγούμενη ρητή συγκατάθεση του παραλήπτη, δηλαδή κάθε μήνυμα spam, είναι παράνομο.

Μοναδική εξαίρεση στα παραπάνω αποτελεί η παράγραφος 3 του ίδιου άρθρου, όπου ορίζεται ότι «Τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεση του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό κατά τη συλλογή των στοιχείων επαφής, καθώς και σε κάθε μήνυμα, σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση». Τέλος, στην παράγραφο 4 του ίδιου άρθρου ορίζεται ότι «Απαγορεύεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, όταν δεν αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και η έγκυρη διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητεί τον τερματισμό της επικοινωνίας».

Στην περίπτωση μηνυμάτων ηλεκτρονικού ταχυδρομείου που αφορούν την εμπορική προώθηση αγαθών ή υπηρεσιών, ο αποστολέας υποχρεούται (σύμφωνα με το Π.Δ 131/2003 που αφορά νομικά ζητήματα υπηρεσιών της κοινωνίας της πληροφορίας στην εσωτερική αγορά) να αναφέρει τον εμπορικό χαρακτήρα του περιεχομένου στο θέμα του μηνύματος.

Οι παραπάνω ρυθμίσεις ισχύουν για τους παραλήπτες που είναι είτε φυσικά είτε νομικά πρόσωπα.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

1. Τι είναι το SPAM;

Το spam είναι ο συνήθης όρος για την αζήτητη ηλεκτρονική επικοινωνία, δηλαδή τα ενοχλητικά μηνύματα που, χωρίς ποτέ να έχετε ζητήσει, κατακλύζουν το λογαριασμό ηλεκτρονικού ταχυδρομείου σας ή το κινητό σας τηλέφωνο διαφημίζοντας διαφόρων ειδών προϊόντα ή υπηρεσίες. Οι αποστολείς μηνυμάτων spam είναι γνωστοί και ως spammers.

2. Ποια προβλήματα δημιουργεί το SPAM;

Το spam υποσκάπτει την εμπιστοσύνη των χρηστών ηλεκτρονικών υπηρεσιών και οδηγεί σε απώλεια χρόνου, πόρων και παραγωγικότητας, τόσο για τους ίδιους τους χρήστες, όσο και για τις επιχειρήσεις. Προβλήματα δημιουργεί επίσης και στους Παρόχους Υπηρεσιών Διαδικτύου (ΠΥΔ), καθώς μπορεί να μειώσει την ποιότητα των παρεχόμενων υπηρεσιών και το χρόνο απόκρισης του δικτύου τους, πλήττοντας έτσι τη διαθεσιμότητα και αξιοπιστία τους. Ενδεικτικά αναφέρεται ότι πάνω από το 70% των μηνυμάτων ηλεκτρονικού ταχυδρομείου σήμερα είναι spam.

Επιπλέον, τα μηνύματα spam, εκτός από ενοχλητικά, μπορεί να είναι προσβλητικά, απατηλά ή ακόμα και επικίνδυνου περιεχομένου. Για παράδειγμα αρκετά μηνύματα spam σήμερα διαφημίζουν πλαστά προϊόντα (π.χ. φαρμακευτικά προϊόντα ή προϊόντα λογισμικού) ως προϊόντα γνωστών εταιρειών, διαδίδουν παραπλανητικές ειδήσεις (όπως π.χ. σχετικά με τη "δύναμη" συγκεκριμένων μετοχών), ή/και προωθούν προϊόντα και υπηρεσίες σεξουαλικού ή/και πορνογραφικού χαρακτήρα. Επίσης, τα μηνύματα spam χρησιμοποιούνται συχνά και ως μέσα μετάδοσης ιών ή άλλων επιβλαβών ή/και κατασκοπευτικών λογισμικών που σκοπεύουν στην "κατάληψη" του υπολογιστή του χρήστη (ή άλλως την μετατροπή του σε zombie computer) και την μετέπειτα χρήση του ως μέσο αποστολής νέων μηνυμάτων spam. Μεγάλη έκταση επίσης έχει πάρει το spam τύπου phishing που στοχεύει στην παραπλάνηση των χρηστών και στην εκμαίευση προσωπικών τους δεδομένων, συχνά με απώτερο σκοπό την απάτη και την απόσπαση χρηματικών ποσών μέσω τραπεζικών λογαριασμών.

3. Γιατί το spam είναι τόσο σύνηθες στο Διαδίκτυο;

Το κόστος αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι πολύ χαμηλό για τους spammers και, επομένως, το ποσοστό ανταπόκρισης των χρηστών δεν χρειάζεται να είναι ιδιαίτερα υψηλό, δεδομένου ότι τελικά κάποιοι χρήστες θα αγοράσουν τα προϊόντα ή τις υπηρεσίες που αυτοί διαφημίζουν. Ενδεικτικά αναφέρεται ότι από σχετική μελέτη που έγινε στην Μεγάλη Βρετανία, 22% των χρηστών είχε αγοράσει τουλάχιστον μία φορά προϊόντα λογισμικού που διαφημίζονταν μέσω spam μηνυμάτων.

4. Το SPAM περιλαμβάνει μόνο μηνύματα ηλεκτρονικού ταχυδρομείου;

Όχι, αν και αυτή είναι η πιο συνήθης περίπτωση. Το spam περιλαμβάνει επίσης μηνύματα που αποστέλλονται μέσω κινητού τηλεφώνου (SMS, MMS), υπηρεσίες στιγμιαίων μηνυμάτων (instant messaging), υπηρεσίες κοινωνικής δικτύωσης (π.χ Facebook), κ.ά.

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

5. Τα μηνύματα SPAM έχουν πάντα εμπορικό περιεχόμενο;

Όχι. Τα μηνύματα spam μπορεί να προωθούν κάθε είδους προϊόντα ή υπηρεσίες. Έτσι ως spam θεωρούνται και μηνύματα προώθησης υπηρεσιών και σκοπών φιλανθρωπικών ιδρυμάτων, σωματείων, ενώσεων, κλπ. Ενδεικτικά αναφέρεται και η 19/2001 Απόφαση της Αρχής που αφορούσε την μετάδοση μέσω ηλεκτρονικού ταχυδρομείου ενός υπερκείμενου συνδέσμου (link) που παρέπεμπε στην ηλεκτρονική εφημερίδα του αποστολέα του μηνύματος. Σημειώνεται επίσης ότι, σύμφωνα με ειδική διακήρυξη της Διεθνούς Συνόδου των Επιτρόπων για την προστασία των προσωπικών δεδομένων του 2005, ακόμα και η πολιτική επικοινωνία οφείλει να συμμορφώνεται με τους κανόνες που ισχύουν για το spam. Η Αρχή έχει εκδώσει τη σχετική Οδηγία 1/2010.

6. Έλαβα το μήνυμα της κάτωθι εικόνας από κάποιον γνωστό. Να ανοίξω τον περιεχόμενο στο μήνυμα σύνδεσμο;

Όχι, επειδή:

- Το μήνυμα δεν έχει θέμα.
- Ο σύνδεσμος που περιέχεται στο μήνυμα παραπέμπει σε «περίεργη ιστοσελίδα».

Επικοινωνήστε με τον γνωστό σας. Ενημερώστε τον για το μήνυμα που λάβατε. Αν δεν το έχει στείλει αυτός, συμβουλέψτε τον να ελέγξει τον υπολογιστή του για ιούς, να ενημερώσει τους άλλους παραλήπτες του μηνύματος σχετικά με το μήνυμα και να αλλάξει το συνθηματικό για το λογαριασμό του ταχυδρομείου του.

Να θυμάστε, επίσης, ότι στο διαδίκτυο μπορεί κάποιος εύκολα να στείλει ένα email προσποιούμενος το γνωστό σας!

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

7. Έλαβα το μήνυμα από κάποιον που μου ζητάει να συμμετάσχω σε μια διαδικασία κληρονομιάς με αντάλλαγμα 50% της κληρονομιάς. Ο αποστολέας μου ζητάει κάποια προσωπικά δεδομένα για να προχωρήσει η διαδικασία της κληρονομιάς. Να στείλω στον αποστολέα τα προσωπικά μου δεδομένα;

Όχι.

Το μήνυμα που λάβατε ανήκει στην κατηγορία μηνυμάτων «advance fee fraud» (μηνύματα, τα οποία θα έπειθαν τον παραλήπτη ενός e-mail ότι, για παράδειγμα, πρέπει να καταβάλει χρήματα για μια διαδικαστική δαπάνη, προκειμένου να παραλάβει κάτι).

Τέτοια μηνύματα συνήθως καταλήγουν στη χρέωση του παραλήπτη με διάφορα τέλη (π.χ. έξοδα κληρονομιάς) χωρίς κανένα χρηματικό όφελος για τον ίδιο.

Καταγγείλτε το παραπάνω μήνυμα σε κατάλληλους φορείς (π.χ. Δ.Η.Ε., Anti-phishing Working Group: http://www.antiphishing.org/).

Μπλοκάρετε τον αποστολέα του μηνύματος ως spammer.

8. Έλαβα μήνυμα από διεύθυνση ηλεκτρονικού ταχυδρομείου, η οποία φαίνεται να ανήκει στην τράπεζα μου. Ο αποστολέας του μηνύματος μού ζητάει να επιβεβαιώσω τα στοιχεία λογαριασμού στο ηλεκτρονικό τραπεζικό σύστημα (e-banking) απαντώντας στο μήνυμα ή επισκεπτόμενος μια ιστοσελίδα που μου προτείνει. Πρέπει να του απαντήσω στο μήνυμα ή να μπω σε αυτή την ιστοσελίδα και να δώσω τα στοιχεία του λογαριασμού μου;

Όχι.

Το μήνυμα που λάβατε ανήκει στην κατηγορία μηνυμάτων phishing (μηνύματα που στοχεύουν στην παραπλάνηση των χρηστών και στην εκμαίευση προσωπικών τους δεδομένων, συχνά με απώτερο σκοπό την απάτη και την απόσπαση χρηματικών ποσών μέσω τραπεζικών λογαριασμών).

Καταγγείλτε το παραπάνω μήνυμα σε κατάλληλους φορείς (π.χ. ΔΗΕ, Anti-phishing Working Group: http://www.antiphishing.org/).

Γνωστοποιείστε το μήνυμα στον υπεύθυνο επεξεργασίας τον οποίο υποδύεται ο αποστολέας.

Μπλοκάρετε τον αποστολέα του μηνύματος ως spammer.

9. Έλαβα ένα μήνυμα που θεωρώ spam, αλλά το ίδιο αναφέρει ότι είναι νόμιμο παραθέτοντας διάφορους λόγους. Είναι;

Όχι.

Πολλές φορές, είτε για να σας παραπλανήσουν είτε από άγνοια, οι αποστολείς διαφημιστικών μηνυμάτων προσθέτουν ένα κείμενο ενημέρωσης στο τέλος του μηνύματος, όπου αναφέρουν ότι το μήνυμα δεν μπορεί να θεωρηθεί spam για διαφόρους λόγους. Επικαλούνται δε και διατάξεις νόμων ή ευρωπαϊκών

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr

οδηγιών. Στις περισσότερες περιπτώσεις παρουσιάζουν μόνο τη «μισή αλήθεια», παραλείποντας τη βασική προϋπόθεση της προηγούμενης συγκατάθεσης.

Το μήνυμα μπορεί να παραθέτει διάφορες δικαιολογίες, όπως για παράδειγμα:

1α	Σκοπός μας είναι η ενημέρωσή σας σχετικά με την ανάπτυξη των ελληνικών εξαγωγών και του διεθνούς εμπορίου γενικότερα. Αυτό το μήνυμα σύμφωνα με το άρθρο 14 του Νόμου 2672/1998 (ΦΕΚ 290 τ.Α) πληροί τις προϋποθέσεις της Ευρωπαϊκής Νομοθεσίας περί διαφημιστικών μηνυμάτων: «Κάθε μήνυμα θα πρέπει να φέρει τα πλήρη στοιχεία του αποστολέα ευκρινώς και θα πρέπει να δίνει στο δέκτη τη δυνατότητα διαγραφής. Εάν το μήνυμα αυτό σας στάλθηκε κατά λάθος ή αν είσαστε στη λίστα μας από λάθος ή αν επιθυμείτε να μην λαμβάνετε πλέον παρόμοια e-mails, σας παρακαλούμε απαντήστε/reply με την λέξη UNSUBSCRIBE στο θέμα ή πατήστε εδώ:
1β	ΣΗΜΑΝΤΙΚΗ ΠΛΗΡΟΦΟΡΙΑ Σύμφωνα με το άρθρο 14 του Νόμου 2672/1998 (ΦΕΚ 290 τ.Α), τα μηνύματα e-mail, για να είναι έγκυρα, θα πρέπει να περιέχουν απαραίτητα: Ονοματεπώνυμο ή επωνυμία (για Νομικό πρόσωπο), ταχυδρομική διεύθυνση κατοικίας, αριθμό τηλεφώνου ή fax, ιδιότητα του χειριστή. Αν τα μηνύματα προέρχονται από υπηρεσία ή Δημόσιο φορέα να περιέχουν επιπλέον θέμα, ημερομηνία, αριθμό πρωτοκόλλου. Το μήνυμα ηλεκτρονικού ταχυδρομείου τεκμαίρεται ότι έχει περιέλθει κανονικά στον λήπτη αν υπάρξει ηλεκτρονική επιβεβαίωση.
2	ΕΝΗΜΕΡΩΣΗ ΣΧΕΤΙΚΑ ΜΕ ΑΥΤΟ ΤΟ ΕΝΗΜΕΡΩΤΙΚΟ EMAIL: Αυτό το e-mail πληροί τις προϋποθέσεις της ευρωπαϊκής νομοθεσίας περί διαφημιστικών μηνυμάτων (Directiva 2002/58/EC του Ευρωπαϊκού Κοινοβουλίου, Relative as A5-270/2001) του Ευρωπαϊκού Κοινοβουλίου και δεν μπορεί να θεωρηθεί spam εφόσον αναγράφονται τα στοιχεία του αποστολέα και οι διαδικασίες διαγραφής από τη λίστα παραληπτών. Αν είσαστε σε αυτή τη λίστα κατά λάθος ή για οποιονδήποτε άλλο λόγο θέλετε να διαγραφεί το e-mail σας, κάντε κλικ εδώ: ΔΙΑΓΡΑΦΗ

Τα παραπάνω στοιχεία, ωστόσο, καθώς και άλλα παρεμφερή, δεν καθιστούν από μόνα τους το μήνυμα νόμιμο. Πιο συγκεκριμένα, επί των παραδειγμάτων οι περιπτώσεις 1α και 1β παραθέτουν νόμο (2672/1998) που αφορά στη διακίνηση εγγράφων με ηλεκτρονικά μέσα για επικοινωνίες με το δημόσιο και σε καμία περίπτωση δεν εφαρμόζεται για τα διαφημιστικά μηνύματα. Στην περίπτωση 2, η Οδηγία 2002/58/ΕΚ είναι αυτή από την οποία έχει προκύψει ο ν. 3471/2006. Σκοπίμως δεν αναφέρεται η βασική προϋπόθεση για την αποστολή διαφημιστικών μηνυμάτων που είναι η συγκατάθεση, ενώ παρουσιάζονται μόνο αυτά που εφαρμόζονται στην περίπτωση που αυτή έχει εξασφαλιστεί, δηλαδή τα στοιχεία του αποστολέα και η διαδικασία διαγραφής. Δείτε αναλυτικά το άρθρο 11 του ν. 3471/2006 και το άρθρο 13 της Οδηγίας 2002/58/ΕΚ (όπως έχει τροποποιηθεί με την Οδηγία 2009/136/ΕΚ).

Vas. Olgas 24 b GR-546 41 Thessaloniki, Greece | T: +30 2310 888 125 | F: +30 2310 887 208 | info@hyphen.gr | www.hyphen.gr