ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΤΜΗΜΑ ΥΠΗΡΕΣΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Εγχειρίδιο Αρ. 1.1

Βασικές Οδηγίες για την Ασφάλεια Πληροφοριών Ηλεκτρονικών Υπολογιστών

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΑΡΑΡΤΗΜΑ IV: ΓΕΝΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ ACTIVE DIRECTORY

ΠΑΡΑΡΤΗΜΑ V: ΙΣΤΟΡΙΚΟ ΠΕΡΙΗΓΗΣΗΣ (HISTORY) - ΜΠΙΣΚΟΤΑΚΙΑ (COOKIES) – ΠΡΟΣΩΡΙΝΗ ΜΝΗΜΗ (CACHE MEMORY)

ΠΑΡΑΡΤΗΜΑ VI: ΣΥΣΤΗΜΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΕΝΟΧΛΗΤΙΚΟΥ/ ΑΝΕΠΙΘΥΜΗΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (ANTI-SPAM SYSTEM)

1. ΕΙΣΑΓΩΓΗ

Το εγχειρίδιο "Βασικές Οδηγίες για την Ασφάλεια Πληροφοριών Ηλεκτρονικών Υπολογιστών" παρέχει πληροφορίες για τις διαδικασίες που πρέπει να ακολουθούν οι λειτουργοί της Δημόσιας Υπηρεσίας για να ελαχιστοποιηθεί ο κίνδυνος απώλειας και διαρροής στοιχείων/πληροφοριών[1]. Το παρόν εγχειρίδιο δίνεται σε όλους τους Δημόσιους Υπαλλήλους και δεν πρέπει να δημοσιοποιείται σε τρίτα άτομα. Η διοίκηση του κάθε Κυβερνητικού Οργανισμού έχει την ευθύνη για την παρακολούθηση της εφαρμογής των προνοιών του εγχειριδίου αυτού.

Η διατήρηση της ασφάλειας της πληροφορίας είναι μια από τις πιο σημαντικές πτυχές ενός Κυβερνητικού Οργανισμού[2], ειδικά για οργανισμούς τόσο μεγάλους και σημαντικούς όπως η Κυβέρνηση μιας χώρας. Η τεχνολογία έχει προχωρήσει τόσο πολύ και έχει εισβάλει δυναμικά στη ζωή μας. Ωστόσο, υπάρχουν ακόμη λειτουργοί της Δημόσιας Υπηρεσίας, οι οποίοι δεν είναι εξοικειωμένοι με τον κόσμο της πληροφορικής και δεν πρέπει ποτέ να θεωρείται ως δεδομένο ότι κάποιος "γνωρίζει". Ως εκ τούτου, το Τμήμα Υπηρεσιών Πληροφορικής (ΤΥΠ) θεώρησε αναγκαία την έκδοση του εγχειριδίου αυτού.

Θα πρέπει να σημειωθεί ότι, η ασφάλεια χαρακτηρίζεται από τη φύση της ως δυναμική και όχι στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η ολοένα βελτιούμενη επιτηδειότητα των 'επιτιθέμενων' (hackers), απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας. Συνεπώς, οι εκάστοτε οδηγίες για την ασφάλεια πληροφοριών θα επανεξετάζονται και θα προσαρμόζονται, όταν αυτό κρίνεται απαραίτητο.

[1] *Το εν λόγω εγχειρίδιο δεν αφορά οδηγίες για διαβαθμισμένες πληροφορίες*

[2] *Ο Κυβερνητικός Οργανισμός αναφέρεται σε Υπουργείο/Τμήμα/ Υπηρεσία της Δημόσιας Υπηρεσίας*

Για σκοπούς πληρότητας αναφέρεται στο σημείο αυτό ότι, ο όρος "ασφάλεια" υποδηλώνει την προστασία από τον κίνδυνο ή την απώλεια και περιλαμβάνει το σύνολο των προληπτικών μέτρων που σχεδιάζονται και αναπτύσσονται από φυσικά και/ή νομικά πρόσωπα για σκοπούς πρόληψης. Η "ασφάλεια" σχετίζεται με όλους τους τομείς της ανθρώπινης δραστηριότητας. Ορισμένοι τέτοιοι τομείς είναι: η φυσική ασφάλεια, η ηλεκτρική ασφάλεια, η ηλεκτρονική ασφάλεια, η εθνική ασφάλεια, κλπ. Μέτρα ασφαλείας ονομάζονται το σύνολο των προληπτικών μέτρων που σχεδιάζει και αναπτύσσει κάποιος για πρόληψη.

1.1. Η έννοια της ασφαλούς πληροφορίας

Πληροφορία είναι οποιοδήποτε γνωσιακό στοιχείο που παράγεται από επεξεργασία δεδομένων. Θεωρείται ένα από τα πιο ουσιώδη περιουσιακά στοιχεία ενός Κυβερνητικού Οργανισμού και συνεπώς πρέπει να προστατεύεται κατάλληλα και να διατηρείται πάντοτε σε χρησιμοποιήσιμη μορφή. Η πληροφορία μπορεί να υπάρχει σε διάφορες μορφές. Μπορεί να είναι τυπωμένη, γραμμένη σε χαρτί ή σε ηλεκτρονική μορφή και να μεταδίδεται είτε με φυσικά μέσα (π.χ. ταχυδρομείο), είτε με ηλεκτρονικά μέσα (ηλεκτρονικό ταχυδρομείο).

Η ασφάλεια των πληροφοριών αναφέρεται στην προστασία της πληροφορίας στην ολότητά της. Για να επιτευχθεί αυτό, είναι απαραίτητο να διασφαλίζεται η ασφάλεια των πληροφοριακών συστημάτων και των μέσων επικοινωνίας. Ως θεμελιώδεις αρχές της «Ασφάλειας της Πληροφορίας» θεωρούνται η ακεραιότητα, η διαθεσιμότητα, η εμπιστευτικότητα, η επικύρωση και η μη αποποίηση ευθύνης, οι οποίες ορίζονται και επιτυγχάνονται ως εξής:

Ακεραιότητα: Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση, χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και στην αποτροπή της πρόσβασης ή/και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια. Συνεπώς, η ακρίβεια και η πληρότητα

των πληροφοριών και των μεθόδων επεξεργασίας τους, διασφαλίζεται μόνο από εξουσιοδοτημένα προγράμματα, κάτω από ένα πλήρως ελεγχόμενο περιβάλλον.

Διαθεσιμότητα: Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, η δικτυακή υποδομή και τα δεδομένα θα είναι στη διάθεση των Χρηστών[3] όποτε απαιτείται η χρήση τους. Μια συνηθισμένη απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα, είναι η επίθεση άρνησης υπηρεσιών, που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευόμενοι πόροι, είτε προσωρινά, είτε μόνιμα. Συνεπώς, αυτό προϋποθέτει ότι, θα πρέπει να τεθούν σε εφαρμογή όλα τα απαραίτητα μέτρα ασφάλειας των συστημάτων και να διασφαλιστεί η σωστή λειτουργία των μεθόδων πρόσβασης σε αυτά.

Εμπιστευτικότητα: Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Συνεπώς, δεν πρέπει να υπάρχει οποιαδήποτε πιθανότητα ή δυνατότητα πρόσβασης σε συστήματα/πληροφορίες ή τροποποίησης/αλλοίωσης πληροφοριών από μη εξουσιοδοτημένα άτομα.

Επικύρωση: Επικύρωση σημαίνει την επιβεβαίωση από τα μέρη (άτομα/συστήματα) που λαμβάνουν μέρος στην ανταλλαγή πληροφοριών. Συνεπώς, η ύπαρξη ασφάλειας των πληροφοριών είναι απαραίτητη ως εγγύηση για τη γνησιότητα και την αυθεντικότητα των πληροφοριών.

Μη Αποποίηση Ευθύνης (non-repudiation): Μη αποποίηση Ευθύνης σημαίνει ότι, κανένας από τους συναλλασσόμενους δεν έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του εκ των υστέρων σε μια ψηφιακή συναλλαγή. Αντιθέτως, η πράξη που έγινε είναι νομικά δεσμευτική και μπορεί να αποδειχθεί στο δικαστήριο. Οι υπηρεσίες μη αποποίησης ευθύνης πρέπει, αν χρειαστεί, να μπορούν να

[3] *Ο όρος χρήστης αφορά Λειτουργούς της Δημόσιας Υπηρεσίας*

αποδείξουν την προέλευση, τη μεταφορά/μετάδοση και την παράδοση των δεδομένων.

Σε περίπτωση ανταλλαγής ηλεκτρονικών μηνυμάτων μεταξύ συναλλασσόμενων, αυτό μπορεί να αποδειχθεί με τους ακόλουθους τρόπους:

- *Ηλεκτρονική υπογραφή* – συνδέεται μονοσήμαντα με τον υπογράφοντα και είναι ικανή να τον ταυτοποιήσει. Δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και συνδέεται με τα δεδομένα κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε αλλοίωση των εν λόγω δεδομένων.

- *Χρονοσφραγίδες (Timestamps)* – επιβεβαιώνουν την ημερομηνία και την ώρα που δημιουργήθηκε ένα ηλεκτρονικό έγγραφο/ψηφιακή πληροφορία/μήνυμα.

Η φυσική ασφάλεια του εξοπλισμού, η ηλεκτρονική ασφάλεια και το ανθρώπινο δυναμικό, αποτελούν τους βασικούς πυλώνες, για την αποτελεσματική προστασία των πληροφοριών που διακινούνται μέσα σε ένα Κυβερνητικό Οργανισμό. Σχετικό είναι το Γράφημα 1 πιο κάτω, όπου φαίνονται όλα τα συστατικά ενός Κυβερνητικού Οργανισμού, τα οποία συμβάλλουν στη διασφάλιση των πληροφοριών.

Γράφημα 1: **Ασφάλεια Δημόσιας Υπηρεσίας**

1.2. Αναγκαιότητα και σκοπιμότητα της ασφάλειας της πληροφορίας

Στη σύγχρονη «ψηφιακή» εποχή η πληροφορία διαδραματίζει καθοριστικό ρόλο σε όλους σχεδόν τους τομείς των καθημερινών δραστηριοτήτων των ατόμων και των Κυβερνητικών οργανισμών.

Η ανάπτυξη της Κοινωνίας της Πληροφορίας, η παγκοσμιοποίηση, η δικτύωση και η μεταφορά των λειτουργιών και υπηρεσιών σε δίκτυα δεδομένων, ενισχύουν ακόμη περισσότερο τη σημασία της πληροφορίας.

Η πληροφορία και οι υποστηρικτικές διαδικασίες, τα πληροφοριακά συστήματα και οι δικτυακές υποδομές, είναι καθημερινά εκτεθειμένα σε κινδύνους και απειλές από διάφορες πηγές όπως απρόβλεπτες βλάβες/ελαττώματα του εξοπλισμού/λογισμικού, κατασκοπεία, δολιοφθορές, υποκλοπές, απάτες φυσικές καταστροφές και ιούς ή ακόμα και από ανθρώπινα λάθη που γίνονται, είτε εκ παραδρομής, είτε λόγω έλλειψης γνώσεων, είτε εσκεμμένα.

Ο Δημόσιος Τομέας συγκεντρώνει, επεξεργάζεται και διαχέει τεράστιες ποσότητες πληροφοριών, οι οποίες είναι πολύ σημαντικές για το συμμετοχικό χαρακτήρα της κοινωνίας και αποτελούν τη βασική πηγή για την κοινωνικοοικονομική δραστηριότητα και την ομαλή λειτουργία της εσωτερικής αγοράς.

Η ασφάλεια της πληροφορίας αποτελεί απαραίτητη προϋπόθεση για την επιχειρησιακή συνέχεια (business continuity), καθώς και για την εύρυθμη και σωστή λειτουργία της Δημόσιας Υπηρεσίας, η οποία διαχειρίζεται μεγάλο όγκο και σημαντικές πληροφορίες όπως, εταιρικές πληροφορίες, περιουσιακά στοιχεία, οικονομικές πληροφορίες, συμβόλαια, προσωπικά δεδομένα και άλλα σημαντικά έγγραφα. Είναι υποχρέωση του Δημόσιου Τομέα να εφαρμόζει τους όρους ασφάλειας στο επίπεδο που κάθε φορά επιβάλλεται, ανάλογα με τη φύση και την κατηγορία των δεδομένων, και να φροντίζει για την ασφάλεια, την ακεραιότητα, την εγκυρότητα, τη διαθεσιμότητα και την αυθεντικότητα των δεδομένων και των ηλεκτρονικών εγγράφων που παράγονται, καταχωρούνται, τηρούνται και διαχειρίζονται.

Διασφαλίζοντας τις πληροφορίες του δημοσίου, οικοδομείται παράλληλα μια νέα σχέση εμπιστοσύνης και αξιοπιστίας ανάμεσα στη Δημόσια Διοίκηση και τον πολίτη.

1.3. Νομοθεσία

- Ο Νόμος 138(Ι) του 2001, Περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου)
- Ο Νόμος 37(Ι) του 2003 που τροποποιεί τον Περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου)
- Ο Νόμος 28(ΙΙΙ) του 2001, Περί Σύμβασης του Συμβουλίου της Ευρώπης για την Προστασία του Ατόμου από την Αυτοματοποιημένη Επεξεργασία Προσωπικών Δεδομένων του 1981.

- Ο Νόμος 30(ΙΙΙ) του 2003, Περί Πρόσθετου Πρωτόκολλου στη Σύμβαση για την Προστασία του Ατόμου από την Αυτοματοποιημένη Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα Κυρωτικός Νόμος του 2003.
- Ο Νόμος 112(Ι) του 2004, Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004, (Μέρος 14).

Επιπρόσθετα βρίσκονται σε ισχύ και οι Γενικές Διατάξεις της Δημόσιας Υπηρεσίας οι οποίες κατά καιρούς τροποποιούνται από το Υπουργικό Συμβούλιο.

1.4. Ιδιοκτησία

Δεδομένα, πληροφορίες, αρχεία και έγγραφα, τα οποία δημιουργούνται, αποστέλλονται, λαμβάνονται και αποθηκεύονται στα συστήματα της Δημόσιας Υπηρεσίας είναι ιδιοκτησία της Κυπριακής Δημοκρατίας.

1.5. Επεξεργασία Δεδομένων

Τα δεδομένα αναφέρονται στο σύνολο διακριτών αντικειμενικών στοιχείων σχετικά με ένα γεγονός ή μία διαδικασία που από μόνα τους δεν έχουν ιδιαίτερη χρησιμότητα.

Οι πληροφορίες αποτελούν συλλογή δεδομένων, τα οποία επεξεργάζεται/ διαχειρίζεται ο Ηλεκτρονικός Υπολογιστής (ΗΥ) και συμπεριλαμβάνει έγγραφα, αρχεία, φωτογραφίες, βίντεο, ηλεκτρονικά μηνύματα, βάσεις δεδομένων και λογισμικά.

Ο κύκλος ζωής των πληροφοριών αποτελείται από τα εξής στάδια: δημιουργία, χρήση, τροποποίηση, αποθήκευση, μεταφορά, διανομή, αντιγραφή, αρχειοθέτηση και καταστροφή.

Οι πληροφορίες είναι πολύ πιο σημαντικές από τα μέσα που χρησιμοποιούνται για την επεξεργασία τους, γι' αυτό και η προστασία τους σε όλα τα στάδια της επεξεργασίας τους είναι απαραίτητη. Συγκεκριμένα οι πληροφορίες πρέπει:

- Να ταξινομούνται και χαρακτηρίζονται ανάλογα με το βαθμό εμπιστευτικότητας τους και να τίθενται οι σχετικοί περιορισμοί χρήσης, κοινοποίησης και επεξεργασίας.
- Να αντιμετωπίζονται με εμπιστευτικότητα και να χρησιμοποιούνται αποκλειστικά για τις εργασίες που προορίζονται.
- Να αποθηκεύονται, όπου είναι δυνατό, σε εξυπηρετητές. Σε αντίθετη περίπτωση, είναι ευθύνη του κάθε υπαλλήλου να δημιουργεί εφεδρικά αντίγραφα (είτε σε CD, είτε σε USB), σε τακτά χρονικά διαστήματα, με τις πληροφορίες που είναι αποθηκευμένες στον Η/Υ του. Σχετικό είναι το ΠΑΡΑΡΤΗΜΑ Ι.

Επίσης:

- Τα CDs/USBs πρέπει πάντοτε να ελέγχονται για ιούς προτού τοποθετηθούν στους υπολογιστές.
- Η επεξεργασία εμπιστευτικών πληροφοριών ή η δακτυλογράφηση κωδικών πρόσβασης πρέπει να γίνεται χωρίς την παρουσία άλλων ατόμων.
- Να αποφεύγεται η αχρείαστη εκτύπωση και αντιγραφή των πληροφοριών, μειώνοντας έτσι τον κίνδυνο να καταλήξουν σε μη εξουσιοδοτημένα άτομα.
- Ο χρήστης πρέπει να βεβαιώνεται σε ποιον εκτυπωτή θα εκτυπώσει και που βρίσκεται ο συγκεκριμένος εκτυπωτής.
- Σε περίπτωση χρήσης εκτυπωτή δικτύου να παραλαμβάνονται άμεσα οι εκτυπώσεις.
- Η αποστολή των εμπιστευτικών πληροφοριών να γίνεται μόνο σε εξουσιοδοτημένα άτομα.
- Να χρησιμοποιούνται συσκευές κατατεμαχισμού (shredders) για την καταστροφή εμπιστευτικών πληροφοριών/εγγράφων.

2. ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

2.1. Γενικές Οδηγίες/Διαδικασίες

- Θα πρέπει να οριστεί Λειτουργός Ασφάλειας σε κάθε Κυβερνητικό Οργανισμό, εκεί όπου δεν υπάρχει, το όνομα του οποίου θα γνωστοποιείται σε όλους τους λειτουργούς του Κυβερνητικού Οργανισμού. Ο Λειτουργός Ασφαλείας θα είναι υπεύθυνος για την επίβλεψη εφαρμογής της πολιτικής ασφάλειας και των οδηγιών που βρίσκονται στο παρόν εγχειρίδιο (σχετικό είναι το Γράφημα 2 πιο κάτω).

- Οι χρήστες έχουν καθήκον και υποχρέωση να ενημερώνουν το Λειτουργό Ασφάλειας του Τμήματός τους όταν εντοπίζουν κάποια αδυναμία στην ασφάλεια ενός συστήματος. Αδυναμίες στην ασφάλεια των συστημάτων συμπεριλαμβάνουν την ασυνήθιστη συμπεριφορά τους π.χ. εργάζεται αργά, εμφανίζει περίεργα μηνύματα, η οποία μπορεί να προκαλέσει διαρροή πληροφοριών ή να είναι ευάλωτα σε απειλές.

  Στη συνέχεια, ο Λειτουργός Ασφάλειας οφείλει να ενημερώσει σχετικά τον Ανώτερο Λειτουργό Ασφάλειας και να αναφέρει τις διορθωτικές ενέργειες που θα κάνει για εξάλειψη της ασφαλιστικής ανεπάρκειας/αδυναμίας του συγκεκριμένου πληροφοριακού συστήματος. Τόσο ο Λειτουργός Ασφάλειας, όσο και ο Ανώτερος Λειτουργός Ασφάλειας, οφείλουν να παρακολουθούν στενά το ζήτημα μέχρι την τελική επίλυσή του.

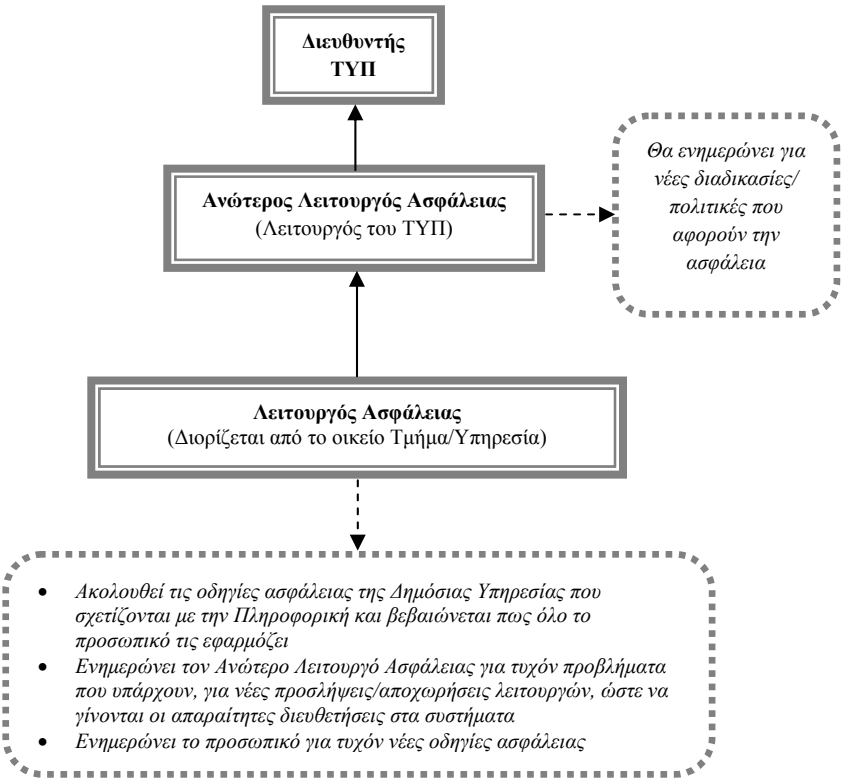
- Οι χρήστες πρέπει να αναφέρουν στο Λειτουργό Ασφαλείας του Τμήματος τους τυχόν παραβιάσεις ή μη-εξουσιοδοτημένη χρήση του Η/Υ, των πληροφοριακών συστημάτων και του ηλεκτρονικού ταχυδρομείου.

- Απαγορεύεται η παράνομη αναπαραγωγή εγγράφων που ανήκουν στην Κυπριακή Δημοκρατία.

- Οι χρήστες δεν πρέπει να μεταφορτώνουν (download), να εγκαθιστούν ή να εκτελούν προγράμματα στους Η/Υ τους, τα οποία δεν είναι εγκεκριμένα από το ΤΥΠ.

- Οι πληροφορίες που βρίσκονται στα συστήματα της Δημόσιας Υπηρεσίας δεν πρέπει να χρησιμοποιούνται για προσωπικούς σκοπούς ή σκοπούς που θεωρούνται παράνομοι σύμφωνα με την Κυπριακή Νομοθεσία.

- Η χρήση Κυβερνητικού φορητού Η/Υ δεν πρέπει να γίνεται από άλλα μη-εξουσιοδοτημένα άτομα (π.χ. φίλοι, μέλη της οικογένειας, κ.α.).



Γράφημα 2

Για να εξασφαλιστεί η ασφάλεια των πληροφοριών θα πρέπει όλο το προσωπικό της Δημόσιας Υπηρεσίας:

- να συνεργάζεται με τους Λειτουργούς Ασφάλειας,
- να τηρεί πιστά και να πράττει όπως προβλέπεται από τις οδηγίες ασφάλειας πληροφοριών, τις οδηγίες χρήσης του εξοπλισμού και τις διαδικασίες της Δημόσιας Υπηρεσίας,
- να οδεύει προς έναν κοινό στόχο για να πετύχει το επιθυμητό αποτέλεσμα - την Ασφάλεια της Δημόσιας Υπηρεσίας,
- να είναι κατάλληλα ενημερωμένο για θέματα ασφάλειας, μέσω εκπαίδευσης/ενημέρωσης και να γνωρίζει τις αρμοδιότητες του και τις ευθύνες του.

2.2. Χρήση Προσωπικού Ηλεκτρονικού Υπολογιστή

Για να εξασφαλιστεί η εύρυθμη λειτουργία του Η/Υ και να διασφαλιστούν οι πληροφορίες που τηρούνται σε αυτόν, ο κάθε λειτουργός της Δημόσιας Υπηρεσίας 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. Περισσότερες πληροφορίες για τους ιούς παρατίθενται στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ.

- 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 στο Λειτουργό Ασφαλείας για καταστροφή, για να αποφευχθεί ο κίνδυνος ανάκτησης των πληροφοριών που τηρούνται σε αυτόν.

- Η εγκατάσταση των λογισμικών γίνεται μόνο από άτομα του ΤΥΠ ή από άτομα/εταιρείες εξουσιοδοτημένες από το ΤΥΠ.

2.3. 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 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 άλλα άτομα.

- Ο χρήστης πρέπει να αλλάζει τον κωδικό πρόσβασής του σε τακτά χρονικά διαστήματα ή όταν υπάρχει υποψία ότι έχει διαρρεύσει σε άλλο μη εξουσιοδοτημένο άτομο.

- Ο κωδικός πρόσβασης δεν πρέπει να αναγράφεται σε χαρτί.

- Ο 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 6 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, κλπ), 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.
  - Ο κωδικός πρόσβασης να μην είναι ο ίδιος με το όνομα χρήστη (username).
  - Να αποφεύγεται ο κωδικός πρόσβασης που 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.
- Για τους χρήστες που είναι συνδεδεμένοι με το Active Directory σχετικό είναι το ΠΑΡΑΡΤΗΜΑ IV.

2.4. Ασφαλής Χρήση του Διαδικτύου και του Ηλεκτρονικού Ταχυδρομείου

Το διαδίκτυο και το ηλεκτρονικό ταχυδρομείο είναι χρήσιμα εργαλεία για την άντληση και ανταλλαγή πληροφοριών. Ωστόσο, η μη σωστή χρήση τους εγκυμονεί πολλούς κινδύνους όπως, υποκλοπή πληροφοριών, παρακολούθηση των κινήσεων του χρήστη κατά την περιήγησή του στο διαδίκτυο, έλλειψη σεβασμού στα προσωπικά δεδομένα, αποστολή ηλεκτρονικών μηνυμάτων σε λανθασμένους χρήστες, κλπ.

Οδηγίες για ασφαλή περιήγηση στο διαδίκτυο και χρήση του ηλεκτρονικού ταχυδρομείου:

- Το διαδίκτυο και το ηλεκτρονικό ταχυδρομείο πρέπει να χρησιμοποιούνται μόνο για σκοπούς εργασίας. Ωστόσο, η περιστασιακή, περιορισμένη και σωστή χρήση του ηλεκτρονικού ταχυδρομείου για προσωπικούς λόγους επιτρέπεται νοουμένου ότι:

  α) δεν επηρεάζει την παραγωγικότητα των Δημοσίων Υπαλλήλων

  β) δεν έχει επίδραση/επίπτωση στην ομαλή λειτουργία του μηχανογραφικού εξοπλισμού του ΤΥΠ ή/και του οικείου Τμήματός/Υπηρεσίας.

- Η λήψη και αποστολή υπηρεσιακών μηνυμάτων γίνεται μόνο διαμέσου του Κυβερνητικού Κόμβου Διαδικτύου, δηλαδή, δεν επιτρέπεται η χρήση ηλεκτρονικού ταχυδρομείου διαμέσου άλλων οργανισμών όπως hotmail, yahoo, gmail κλπ.

- Να αποφεύγεται η λειτουργία της αυτόματης σύνδεσης, εκτός και αν ο Η/Υ βρίσκεται σε ασφαλή χώρο όπου κανείς άλλος δεν μπορεί να έχει πρόσβαση.

- 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). Σχετικό είναι το ΠΑΡΑΡΤΗΜΑ V.

- 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, διατηρώντας παράλληλα και την εμπιστευτικότητα του μηνύματος.

- Η αποστολή μαζικών ηλεκτρονικών μηνυμάτων (bulk emails) σε ομάδες ατόμων, όπου τα στοιχεία τους είναι ορατά από όλους τους παραλήπτες, μπορεί να θεωρηθεί 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).

- Ο χρήστης πρέπει να βεβαιώνεται ότι το ηλεκτρονικό μήνυμα που θα στείλει απευθύνεται στο σωστό παραλήπτη με τη σωστή ηλεκτρονική διεύθυνση.

- Σε περίπτωση αποχώρησης/αφυπηρέτησης κάποιου υπαλλήλου από τη Δημόσια Υπηρεσία, το οικείο Τμήμα/Υπηρεσία πρέπει να ειδοποιεί γραπτώς το ΤΥΠ για να διαγράψει το ηλεκτρονικό του ταχυδρομείο. Ο υπάλληλος, προτού αποχωρήσει/αφυπηρετήσει, έχει την ευθύνη να μεταφέρει στον προϊστάμενό του τα ηλεκτρονικά μηνύματα, τα οποία κρίνονται αναγκαία.

- **Απαγορεύεται:**

  - Η εγκατάσταση λογισμικών 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 αισχρών μηνυμάτων με περιεχόμενο που μπορεί να θεωρηθεί άσεμνο, προσβλητικό, δυσφημιστικό, ανάρμοστο ή και εξευτελιστικό (π.χ. σεξουαλικό περιεχόμενο, κακολογίες ρατσιστικού ή εθνικιστικού περιεχομένου, κ.λπ.).

- Η αποστολή μηνυμάτων τύπου αλυσίδας (Chain mail) ή ανεπιθύμητων μηνυμάτων διαφημιστικού περιεχομένου ή προωθητικού περιεχομένου σε χρήστες που δεν έχουν αποδεχτεί τη λήψη τέτοιου είδους μηνύματος (Spam mail). Όσον αφορά τη λήψη ηλεκτρονικών μηνυμάτων, το ΤΥΠ έχει εγκαταστήσει εξειδικευμένο λογισμικό αντιμετώπισης ανεπιθύμητων/ενοχλητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου («Το Σύστημα»). Σχετικό είναι το ΠΑΡΑΡΤΗΜΑ VI.

- Η αποστολή εμπιστευτικών μηνυμάτων/πληροφοριών μέσω ηλεκτρονικού ταχυδρομείου ή/και του διαδικτύου.
- Η καταχώρηση των κυβερνητικών ηλεκτρονικών διευθύνσεων σε διαδικτυακό τόπο που δε σχετίζονται με την εργασία του υπαλλήλου.
- Η απάντηση σε ανεπιθύμητη αλληλογραφία (junk mail). Αντιθέτως, τέτοια μηνύματα πρέπει να διαγράφονται αμέσως.

2.5. Απομακρυσμένη Πρόσβαση σε Ηλεκτρονικό Ταχυδρομείο

- Η σύνδεση με το δίκτυο της Δημόσιας Υπηρεσίας (Κυβερνητικό Δίκτυο Δεδομένων) για λήψη/αποστολή ηλεκτρονικών μηνυμάτων εκτός του εργασιακού χώρου επιτρέπεται **μόνο** κατόπιν έγκρισης από το Διευθυντή του οικείου Τμήματός/Υπηρεσίας.
- Μόνο λειτουργοί του ΤΥΠ μπορούν να εγκαταστήσουν τα απαραίτητα λογισμικά και εξοπλισμό για να υπάρχει σύνδεση του χρήστη με το Κυβερνητικό Δίκτυο Δεδομένων εκτός του εργασιακού χώρου.
- Απαγορεύεται η σύνδεση των εταιρειών, που παρέχουν λειτουργική υποστήριξη στα διάφορα Πληροφοριακά Συστήματα, στο Κυβερνητικό Δίκτυο Δεδομένων.

2.6. 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 σε κυβερνητικούς χώρους 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 Δημόσιος Υπάλληλος 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.).

2.7. 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 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 το Λειτουργό Ασφάλειας του Τμήματός του ή τον Ανώτερο Λειτουργό Ασφάλειας του ΤΥΠ.
- 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 των λειτουργών της Δημόσιας Υπηρεσίας να ενημερώνουν άμεσα τους Λειτουργούς Ασφάλειας ή τον Ανώτερο Λειτουργό Ασφάλειας 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.

3. ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (PRIVACY)

- Η φύλαξη προσωπικών αρχείων/εγγράφων/πληροφοριών στους κυβερνητικούς Η/Υ ή/και εξυπηρετητές πρέπει να αποφεύγεται.
- Η προστασία των προσωπικών πληροφοριών ή/και μηνυμάτων που λαμβάνει ο κάθε Δημόσιος Υπάλληλος είναι δική του ευθύνη.
- Οι πληροφορίες που τηρούνται/αποθηκεύονται στα ημερολογιακά αρχεία (log files) των συστημάτων και του δικτυακού εξοπλισμού θα πρέπει να χρησιμοποιούνται **μόνο** για τη συντήρηση, την ανίχνευση προβλημάτων και την επίβλεψη της ασφάλειας πληροφοριών.
- Οι Δημόσιοι Υπάλληλοι είναι υποχρεωμένοι να μην κοινοποιούν οποιαδήποτε προσωπικά μηνύματα ή πληροφορίες που έρχονται στην αντίληψή τους, λόγω της φύσης της εργασίας που εκτελούν (π.χ. διαχειριστές συστημάτων).
- Η πλοήγηση στο διαδίκτυο και η χρήση μηχανών αναζήτησης εποπτεύονται για λόγους διασφάλισης της αποτελεσματικότητας και της σωστής χρήσης των συστημάτων. Οι χρήστες πρέπει να καταγγέλλουν στο Λειτουργό Ασφάλειας οποιαδήποτε αχρείαστη παρέμβαση ή παρενόχληση από τους εποπτεύοντες.
- Όλοι οι Δημόσιοι Υπάλληλοι είναι υποχρεωμένοι όταν αποχωρούν από την εργασία τους, να σβήνουν όλες τις συσκευές που έχουν υπό την ευθύνη τους είτε είναι Ηλεκτρονικός Υπολογιστής είτε εκτυπωτής κ.τ.λ.

3.1. Επιπτώσεις

Η παραβίαση των νόμων, κανονισμών και οδηγιών της Δημόσιας Υπηρεσίας μπορεί να οδηγήσει, ανάλογα με το παράπτωμα, σε αφαίρεση των δικαιωμάτων πρόσβασης του χρήστη στα συστήματα, στην καταβολή αποζημιώσεων, ή/και επιβολή άλλων μέτρων ως οι πρόνοιες του Περί Δημόσιας Υπηρεσίας Νόμου του 1990 (Ν. 1/1990).

4. ΒΙΒΛΙΟΓΡΑΦΙΑ

1. http://el.wikipedia.org
2. http://www.opengov.gr
3. http://eur-lex.europa.eu
4. http://en.wikipedia.org
5. http://www.otenet.gr
6. http://www.bankofgreece.gr
7. http://support.microsoft.com
8. http://www.global-tech.gr
9. http://help.pathfinder.gr
10. http://www.trainmor-knowmore.eu

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ Ι

ΔΙΑΔΙΚΑΣΙΑ ΤΗΡΗΣΗΣ ΕΦΕΔΡΙΚΩΝ ΑΝΤΙΓΡΑΦΩΝ

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.

Η διαδικασία για τη δημιουργία αντιγράφων ασφαλείας του Ηλεκτρονικού Υπολογιστή είναι η ακόλουθη:

1. Επιλογή του μέσου για εγγραφή των αντιγράφων. Οι πιο πιθανές επιλογές είναι το CD-R/DVD-R, σκληροί δίσκοι (εσωτερικοί ή εξωτερικοί), όπως και USBs. Σε καμία περίπτωση να μη δημιουργούνται τα αντίγραφα στο δίσκο στον οποίο βρίσκονται εγκαταστημένα τα Windows.

2. Επιλογή του σωστού λογισμικού για δημιουργία αντιγράφων ασφαλείας. Στα Win 7 όπως και σε όλες τις άλλες εκδόσεις των Windows υπάρχει ειδική εφαρμογή για το backup.
   Windows XP: Start>Programs>Accessories>System Tools>Backup
   Windows Vista: Start>Control Panel>System and Maintenance>Backup and Restore Center
   Windows 7: Start> Control Panel>System and Maintenance>Backup and Restore

3. Πέρα από τα πιο πάνω λογισμικά, ο χρήστης θα μπορούσε να επιλέξει οποιοδήποτε άλλο λογισμικό ανοικτού κώδικα για τη δημιουργία αντιγράφων ασφαλείας.

Η πιο συνηθισμένη διαδικασία τήρησης εφεδρικών αντιγράφων ασφαλείας είναι η αντιγραφή του Φακέλου «My Documents» και του ηλεκτρονικού ταχυδρομείου επί καθημερινής βάσης σε ένα USB με την κατάλληλη χωρητικότητα.

ΕΝΗΜΕΡΩΣΗ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ (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.

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.

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**.

Σε περίπτωση που η ενημέρωση του λειτουργικού συστήματος δεν είναι αυτόματη, ο υπάλληλος οφείλει να ακολουθεί την προαναφερθείσα διαδικασία τουλάχιστο μία φορά την εβδομάδα.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ

ΙΟΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

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).

<u>Συμπτώματα Ηλεκτρονικού Υπολογιστή σε περίπτωση μόλυνσης από ιό (Virus)</u>

- 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.*

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 λειτουργία του προγράμματος antivirus. Η συγκεκριμένη λειτουργία της απόκρυψης του ιού από το antivirus (αντι-antivirus) 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.

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 τους Λειτουργούς Ασφάλειας του Τμήματός τους. Σε ορισμένους Κυβερνητικούς Οργανισμούς η ανανέωση των προγραμμάτων ανίχνευσης/ προστασίας ιών (antivirus programs) γίνεται αυτόματα (κεντρικά) σε τακτά χρονικά διαστήματα, έτσι οι χρήστες δε χρειάζεται να κάνουν οποιαδήποτε ενέργεια.*

ΓΕΝΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ ACTIVE DIRECTORY

Το Active Directory είναι μια ειδική εφαρμογή της Microsoft, η οποία επιτρέπει την αποθήκευση και την οργάνωση πληροφορίας σχετικά με τους χρήστες του Κυβερνητικού Δικτύου της Δημόσιας Υπηρεσίας.

Η υπηρεσία καταλόγου Active Directory διαδραματίζει πολλούς ρόλους, λειτουργώντας ως σπονδυλική στήλη της κατανεμημένης ασφάλειας και ως κεντρικός αποθηκευτικός χώρος για πληροφορίες που αφορούν ολόκληρη την τεχνική υποδομή του Κυβερνητικού Οργανισμού.

Η δημιουργία ενιαίου Active Directory για όλο το Κυβερνητικό Δίκτυο ενισχύει την ασφάλεια του δικτύου και των προσωπικών υπολογιστών, παρέχοντας:

- Κεντρική πιστοποίηση της ταυτότητας των χρηστών (authentication).
- Ελεγχόμενη πρόσβαση στους πόρους δικτύου του Κυβερνητικού Οργανισμού.
- Ελεγχόμενη εγκατάσταση λογισμικού στους μικροϋπολογιστές.
- Αποτελεσματική εφαρμογή των πολιτικών ασφαλείας από το κέντρο (ΤΥΠ).
- Τεχνολογική ομοιομορφία σε σχέση με τα λογισμικά που χρησιμοποιούνται στη Δημόσια Υπηρεσία.

Κωδικοί Πρόσβασης

Κανόνες αλλαγής κωδικού πρόσβασης:

- Τήρηση ιστορικού κωδικού πρόσβασης: 3 τελευταίοι κωδικοί
- Μέγιστη Διάρκεια ζωής κωδικού: 60 ημέρες
- Ελάχιστη Διάρκεια ζωής κωδικού: 1 μέρα
- Ελάχιστος αριθμός χαρακτήρων: 8
- Ο κωδικός πρόσβασης πρέπει να περιέχει τουλάχιστον έναν αριθμό, ένα κεφαλαίο γράμμα και έναν ειδικό χαρακτήρα.
- Δεν επιτρέπεται η χρήση του ονόματος ή/και του επιθέτου του χρήστη.

Γενικές οδηγίες

- Για τους χρήστες του Active Directory, η ενημέρωση του λειτουργικού συστήματος Windows και του λογισμικού Antivirus Panda γίνεται αυτόματα και δε χρειάζεται η παρέμβαση του χρήστη.
- Ο χρήστης δεν μπορεί να χρησιμοποιήσει τον ίδιο κωδικό πρόσβασης για τρείς συνεχόμενες περιόδους.
- Δεν επιτρέπεται η εγκατάσταση καινούργιων Λογισμικών.

ΙΣΤΟΡΙΚΟ ΠΕΡΙΗΓΗΣΗΣ (HISTORY) - ΜΠΙΣΚΟΤΑΚΙΑ (COOKIES) – ΠΡΟΣΩΡΙΝΗ ΜΝΗΜΗ (CACHE 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.

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.

<u>Διαγραφή Ιστορικού Περιήγησης – Cookies – Προσωρινής Μνήμης</u>

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 Preserve 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 το Λειτουργό Ασφάλειας του Τμήματός σας.*

ΠΑΡΑΡΤΗΜΑ VI

ΣΥΣΤΗΜΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΕΝΟΧΛΗΤΙΚΟΥ/ΑΝΕΠΙΘΥΜΗΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (ANTI-SPAM SYSTEM)

Το ΤΥΠ έχει εγκαταστήσει εξειδικευμένο λογισμικό αντιμετώπισης ανεπιθύμητων/ενοχλητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου («το Σύστημα»).

Το Σύστημα ελέγχει όλα τα εισερχόμενα μηνύματα προς το Κυβερνητικό Σύστημα Ηλεκτρονικού Ταχυδρομείου και για κάθε μήνυμα λαμβάνει ένα από τα ακόλουθα μέτρα:

(α) Μήνυμα που κρίνεται με βεβαιότητα από το Σύστημα ως ενοχλητικό/ανεπιθύμητο ηλεκτρονικό ταχυδρομείο απορρίπτεται και δεν προωθείται στον παραλήπτη, χωρίς αυτός να λαμβάνει οποιαδήποτε ενημέρωση.

(β) Μήνυμα που κρίνεται ως πιθανό ενοχλητικό/ανεπιθύμητο ταχυδρομείο κατακρατείται σε απομόνωση από το Σύστημα και το Σύστημα αποστέλλει αυτόματα προς τον παραλήπτη σχετικό ενημερωτικό μήνυμα.

(γ) Μήνυμα που δεν εμπίπτει σε καμιά από τις δύο προηγούμενες περιπτώσεις προωθείται κανονικά στον παραλήπτη του.

Στην περίπτωση ηλεκτρονικού ταχυδρομείου που εμπίπτει στο (β) πιο πάνω, το μήνυμα που αποστέλλεται αυτόματα από το Σύστημα έχει τις ακόλουθες επιλογές:

(α) “DELETE”: Με την επιλογή αυτή το ύποπτο μήνυμα διαγράφεται από το χώρο απομόνωσης που είχε αποθηκευτεί προσωρινά και ο παραλήπτης δεν λαμβάνει το μήνυμα.

(β) “RELEASE”: Με την επιλογή αυτή το ύποπτο μήνυμα διαβιβάζεται στα εισερχόμενα του παραλήπτη του μηνύματος και ο αποστολέας του μηνύματος καταχωρείται στο “White List” που τηρείται από το Σύστημα, για το συγκεκριμένο παραλήπτη, ώστε μελλοντικά μηνύματα από το συγκεκριμένο

αποστολέα προς το συγκεκριμένο παραλήπτη να μην θεωρούνται ύποπτα από το Σύστημα και να προωθούνται κανονικά στον παραλήπτη τους.

Επισημαίνεται ότι οι ίδιες επιλογές (DELETE, RELEASE) υπάρχουν ως Web Actions και ως Email Actions. Σε περίπτωση που για οποιοδήποτε λόγο οι επιλογές κάτω από Web Actions δεν ανταποκρίνονται, τότε πρέπει να χρησιμοποιούνται οι αντίστοιχες επιλογές κάτω από Email Actions.

Το ενημερωτικό μήνυμα που αποστέλλεται αυτόματα από το Σύστημα στον παραλήπτη έχει ως ακολούθως:

The email(s) below has been detected as SPAM (Unsolicited bulk email) and has been quarantined for security reasons.

Date:	From:	Subject:	Web Actions:	Email Actions:
Thu, 15 Oct 2009 10:36:31	"Lufthansa" <newsletter@flyaway.rjs0.com>	Whether America or Asia - act fast or lose out	Release Delete	Release Delete

Web Actions:
* If you want to receive the email click on **Release**.
* If you DO NOT want to receive the email and permanently delete it, click on **Delete**
* If you want to delete ALL of the above then click Delete all.

Email Actions:
* Click on **Release** link to send an email to have the message sent to your **inbox**.
* Click on **Delete** link to send an email to delete the message from your **quarantine**.

Other:
To view your entire quarantine inbox or manage your preferences, Click Here
This is an automated message from the Government Internet Node - Dept. of information Technology Services (DITS)
Note: The sender of a released message will be added to your white list.