



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ



ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΑΞΙΟΛΟΓΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Προτεινόμενη Τεκμηρίωση Υποδομών

Αρχείο Αλλαγών

Έκδοση	Ημερομηνία	Περιγραφή	Ενότητες
1.0	09/03/2015	1 ^η Έκδοση	
1.5	08/05/2015	1 ^η Έκδοση, Υποέκδοση 5	
2	25/01/2016	2 ^η Έκδοση	
2.1	26/03/2018	2 ^η Έκδοση, Υποέκδοση 1	
2.2	09/07/2019	2 ^η Έκδοση, Υποέκδοση 2	

Περιεχόμενα

1. Συντομογραφίες - Όροι	4
2. Σχέδιο Ασφάλειας	5
2.1 Τεκμηρίωση Υποδομών:	5
2.2. Συμπληρωματική Τεκμηρίωση Λειτουργικών Συστημάτων:	6
2.2.1. Λειτουργικό σύστημα Microsoft Windows	6
2.2.2. Λειτουργικό σύστημα Linux	6
2.2.3. Λειτουργικό σύστημα Apple macOS	6
2.3. Τεκμηρίωση Χρηστών (Διαχειριστές, Χρήστες, Δικαιώματα χρηστών):	7
2.4. Τεκμηρίωση Πρόσβασης Χρηστών:	7
2.5. Τεκμηρίωση Εφεδρικής Αποθήκευσης και Ανάκτησης:	8
2.6. Τεκμηρίωση Μέτρων Ασφάλειας και Προστασίας των Υποδομών:	8
2.7. Τεκμηρίωση Παρακολούθησης Ορθής Λειτουργίας των Υποδομών:	9
3. Σχέδιο Επιχειρησιακής Συνέχειας και Ανάκτησης από Καταστροφή	10
4. Συμβόλαια Συντήρησης και Τεχνικής Υποστήριξης με τρίτες εταιρίες	11
5. Πολιτική Ορθής Χρήσης και Δεοντολογίας	12
6. Πιστοποιήσεις από ανεξάρτητους φορείς	13

1. Συντομογραφίες - Όροι

- **ΕΟΦ**: Εγκεκριμένος Οικονομικός Φορέας
- **ΑΕΟ**: Authorised Economic Operator
- **υ-ΕΟΦ**: Υποψήφιος ΕΟΦ
- **Εταιρία**: η εταιρία που αιτείται Άδεια ΕΟΦ ή Άδεια Εκτελωνισμού στον Οριζόμενο Τόπο
- **ΠΣ**: Πληροφοριακό Σύστημα
- **ΠΑ-ΠΣ**: Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων
- **ΣΥΑ-ΠΣ**: Σχέδιο Υλοποίησης Ασφάλειας Πληροφοριακών Συστημάτων
- **ΠΟΧΔ-ΠΣ**: Πολιτική Ορθής Χρήσης και Δεοντολογίας των Πληροφοριακών Συστημάτων
- **ΣΕΣΑ-ΠΣ**: Σχέδιο Επιχειρησιακής Συνέχειας και Ανάκτησης από Καταστροφή των Πληροφοριακών Συστημάτων
- **BCP**: Business Continuity Plan
- **DRP**: Disaster Recovery Plan
- **SLA**: Service Level Agreement
- **VLAN**: Virtual Local Area Network
- **NDA**: Non-Disclosure Agreement
- **RDP**: Remote Desktop Protocol
- **VNC**: Virtual Network Computing
- **NAT**: Network Addresss Translation

2. Σχέδιο Ασφάλειας

Το Σχέδιο Ασφάλειας εμπεριέχει την **Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων** (ΠΑ-ΠΣ) και το **Σχέδιο Υλοποίησης Ασφάλειας Πληροφοριακών Συστημάτων** (ΣΥΑ-ΠΣ), και απαντάει στο σύνολο των ερωτήσεων του Ερωτηματολογίου Αξιολόγησης της Ασφάλειας Πληροφοριακών Συστημάτων. Συνεπώς, όλες οι ερωτήσεις του Ερωτηματολογίου θα πρέπει να παραπέμπουν για αναλυτική απάντηση σε κάποια παράγραφο του Σχεδίου Ασφάλειας. Διευκρινίζεται ότι τα παραπάνω μπορεί να περιέχονται ως πληροφορία και σε περισσότερα εσωτερικά έγγραφα, τα οποία συνολικά συνθέτουν το Σχέδιο Ασφάλειας της εταιρίας σας.

Το **Σχέδιο Ασφάλειας** ενδεικτικά περιέχει τα παρακάτω:

2.1 Τεκμηρίωση Υποδομών:

- Πλήρη περιγραφή του computer room ή του χώρου εγκατάστασης (φυσική πρόσβαση, προστασία χώρου, ασφάλεια συστημάτων, ρεύματα, εναλλακτική παροχή ηλ. ρεύματος, κλιματισμός κ.λπ.).
- Πλήρες και αναλυτικό Διάγραμμα Αρχιτεκτονικής Δικτύου που να περιλαμβάνει:
 - Δικτυακές συσκευές, servers, σταθμούς εργασίας. Για κάθε δικτυακή συσκευή να εμφανίζεται ο αριθμός των Interfaces που διαθέτει,
 - VLANs,
 - Συνδέσεις με Internet, τρόπος με τον οποίο επιτυγχάνεται η σύνδεση στο Internet (π.χ. leased line, adsl, μικροκυματική ζεύξη κ.α.),
 - Συνδέσεις με απομακρυσμένα δίκτυα.
- Πλήρη περιγραφή του τοπικού δικτύου των σταθμών εργασίας. Υπάρχει Primary Domain Controller; Υπάρχει Active Directory;
- Λίστα εξοπλισμού, η οποία να περιέχει για την κάθε συσκευή:
 - Κατασκευαστή, μοντέλο, serial numbers, κύρια χαρακτηριστικά,
 - Τύπο συσκευής, ρόλους που εξυπηρετεί, s/w που τρέχει (λειτουργικό σύστημα, έτοιμα πακέτα λογισμικού, εφαρμογές),
 - Εγγύηση, συντήρηση/υποστήριξη, αντίστοιχο συμβόλαιο.
- Λίστα λογισμικού (λειτουργικών συστημάτων, έτοιμων πακέτων λογισμικού, εφαρμογών) που για κάθε πακέτο να περιέχει:
 - Κατασκευαστή, έκδοση, serial numbers, κωδικούς προϊόντος (software keys),
 - Συσκευή όπου είναι εγκατεστημένο,
 - Εγγύηση, συντήρηση/υποστήριξη, αντίστοιχο συμβόλαιο.
- Λίστα προμηθευτών, κατασκευαστών, συνεργατών (που υποστηρίζουν το ΠΣ) για το hardware και το software, με στοιχεία επικοινωνίας (για περίπτωση προβλήματος).
- Κατηγοριοποίηση πόρων Πληροφοριακού Συστήματος (ΠΣ) ως προς τη σπουδαιότητά τους για την εύρυθμη λειτουργία της εταιρίας.
- Κατηγοριοποίηση περιβαλλόντων Πληροφοριακού Συστήματος ως προς το είδος λειτουργίας τους (παραγωγικό περιβάλλον, περιβάλλον ανάπτυξης, test περιβάλλον).

2.2. Συμπληρωματική Τεκμηρίωση Λειτουργικών Συστημάτων:

2.2.1. Λειτουργικό σύστημα Microsoft Windows

Στην περίπτωση χρήσης εκδόσεων του λειτουργικού συστήματος Microsoft Windows, **θα πρέπει να ληφθεί σοβαρά υπόψη** ο επίσημος κύκλος ζωής υποστήριξης της κάθε έκδοσης. Η πληροφορία αυτή μπορεί να ανακτηθεί από τον παρακάτω σύνδεσμο:

<https://support.microsoft.com/en-us/lifecycle/search>.

Όταν για έκδοση του συγκεκριμένου λειτουργικού έχει ανακοινωθεί επίσημη ημερομηνία τέλους υποστήριξης (end-of-support), τότε δεν υπάρχουν πλέον διαθέσιμες αυτόματες ενημερώσεις (automatic updates). Το γεγονός αυτό σημαίνει ότι τα συστήματα αυτά είναι εκτεθειμένα σε κακόβουλες ενέργειες. Όπως άλλωστε επισημαίνεται και στον παρακάτω σύνδεσμο (<http://windows.microsoft.com/en-us/windows/end-support-help>): «*If you continue to use Windows after support ends, your computer will still work but it might become more vulnerable to security risks and viruses*».

Όταν κατά την ημερομηνία της Αξιολόγησης της αίτησης η ημερομηνία τέλους υποστήριξης μιας χρησιμοποιούμενης έκδοσης του λειτουργικού συστήματος έχει παρέλθει ή πρόκειται να παρέλθει πολύ σύντομα (και σίγουρα εντός των προθεσμιών που έχουν τεθεί από την εκάστοτε Τελωνειακή Περιφέρεια για την Αξιολόγηση), **τότε η εταιρία οφείλει να προχωρήσει σε αναβάθμιση σε νεώτερη έκδοση στους σταθμούς εργασίας ή στους εξυπηρετητές όπου είναι εγκατεστημένη η εν λόγω έκδοση.**

Σε περίπτωση που ο αριθμός των παραπάνω servers/workstations είναι σημαντικός, τότε αρκεί να επιδειχθεί ο χρονοπρογραμματισμός της εργασίας αναβάθμισης (με σαφή χρονοδιαγράμματα), η οποία σε μεταγενέστερο στάδιο θα ελεγχθεί για την επιτυχή ολοκλήρωσή της.

Σημειώνεται ότι για παλαιότερες εκδόσεις του λειτουργικού συστήματος Microsoft Windows ισχύουν οι παρακάτω ημερομηνίες τέλους υποστήριξης::

- **Windows 2003 Server**, 14 Ιουλίου 2015 (βλ. [εδώ](#))
- **Windows XP**, 8 Απριλίου 2014 (βλ. [εδώ](#) και [εδώ](#))
- **Windows 2000 Pro**, 13 Ιουλίου 2010 (βλ. [εδώ](#))
- **Windows NT4 SP6a**, 31 Δεκεμβρίου 2004 (βλ. [εδώ](#))

2.2.2. Λειτουργικό σύστημα Linux

Στην περίπτωση χρήσης εκδόσεων του λειτουργικού συστήματος Linux, και ανάλογα με τη χρησιμοποιούμενη διανομή Linux, **θα πρέπει να ληφθεί σοβαρά υπόψη** ο επίσημος κύκλος ζωής υποστήριξης της κάθε έκδοσης. Η πληροφορία αυτή μπορεί να ανακτηθεί από τον παρακάτω σύνδεσμο:

<https://linuxlifecycle.com/>.

2.2.3. Λειτουργικό σύστημα Apple macOS

Στην περίπτωση χρήσης εκδόσεων του λειτουργικού συστήματος macOS της Apple, η πολιτική της Apple επιβάλλει γενικά την υποστήριξη όλων των προηγούμενων εκδόσεων, ανεξαρτήτως προϊόντος (συσκευής) στο οποίο είναι εγκατεστημένα, αρκεί το εκάστοτε hardware να μπορεί να υποστηρίξει την κάθε έκδοση του λειτουργικού συστήματος. Σε περίπτωση που η συσκευή Apple δεν υποστηρίζει μια νέα έκδοση του λειτουργικού macOS, τότε η συσκευή εξακολουθεί και λειτουργεί με την προηγούμενη έκδοση.

Ωστόσο, θα πρέπει να επιδεικνύεται πάντοτε η ενημέρωση των χρησιμοποιούμενων λειτουργικών συστημάτων με τα τελευταία διαθέσιμα διορθωτικά patches ή updates.

Περισσότερες πληροφορίες μπορούν να ανακτηθούν από τους παρακάτω συνδέσμους:

<https://en.wikipedia.org/wiki/MacOS#Versions>

<https://support.apple.com/en-us/HT201686>.

2.3. Τεκμηρίωση Χρηστών (Διαχειριστές, Χρήστες, Δικαιώματα χρηστών):

- Αρμόδιος Υπεύθυνος του ΠΣ, ρόλο στον υ-ΕΟΦ.
- Λίστα με τους υπεύθυνους υπαλλήλους του υ-ΕΟΦ ανά υποσύστημα/εφαρμογή του ΠΣ, με ρόλο ανά υπάλληλο και τηλ. επικοινωνίας.
- Αριθμό χρηστών του ΠΣ, αριθμό transactions που καταγράφονται ανά ημέρα στο ΠΣ, αριθμό παραστατικών που διακινούνται ανά ημέρα.
- Λίστα με τα Static IPs των χρηστών, τα δικαιώματά τους στις εφαρμογές και στα συστήματα (ως αναφορά για χρήση από τον υ-ΕΟΦ, όχι για τις ανάγκες της Αξιολόγησης).

2.4. Τεκμηρίωση Πρόσβασης Χρηστών:

- Πολιτική απόδοσης usernames και passwords στους χρήστες, τόσο για τους σταθμούς εργασίας όσο και για τις εφαρμογές:
 - Πολιτική δημιουργίας έγκυρου και ισχυρού password (μήκος, κεφαλαία-πεζά, ειδικοί χαρακτήρες κ.λπ),
 - Αλλαγή του password του κάθε χρήστη σε τακτά χρονικά διαστήματα, για λόγους ασφαλείας,
 - Φόρμες Δημιουργίας / Μεταβολής / Διαγραφής χρήστη στο ΠΣ.
- Πολιτική απόδοσης δικαιωμάτων πρόσβασης των χρηστών στα συστήματα και τις εφαρμογές.
- Διαδικασίες πρόσβασης των διαχειριστών και των χρηστών στα συστήματα και τις εφαρμογές.
- Διαδικασίες πρόσβασης τρίτων (συνεργάτες, πελάτες, εταιρίες υποστήριξης του ΠΣ) στους φυσικούς πόρους και τα δεδομένα του ΠΣ.
- Πολιτική απομακρυσμένης πρόσβασης σε συστήματα και εφαρμογές:
 - Ποιοι έχουν δικαίωμα απομακρυσμένης πρόσβασης (υπάλληλοι, συνεργάτες, πελάτες, εταιρίες υποστήριξης του ΠΣ);
 - Ποιο VNC software χρησιμοποιείται (TeamViewer, Remote Desktop Connection, άλλο);
 - Ποιο RDP software χρησιμοποιείται (Remote Desktop Connection, άλλο);
 - Ποια μέτρα ασφαλείας λαμβάνονται και υλοποιούνται στις δικτυακές συσκευές, τους σταθμούς εργασίας, τους servers και τις εφαρμογές; Υπάρχει κεντρική πολιτική;

- Απαιτείται προηγούμενη εξουσιοδότηση και ενεργοποίηση της δυνατότητας απομακρυσμένης πρόσβασης στο ΠΣ;
- Διαδικασίες ασύρματης πρόσβασης:
 - Ασύρματη πρόσβαση διαχειριστών και χρηστών,
 - Ασύρματη πρόσβαση επισκεπτών.

2.5. Τεκμηρίωση Εφεδρικής Αποθήκευσης και Ανάκτησης:

- Πολιτική Backup και Restore συστημάτων, εφαρμογών και δεδομένων:
 - Συστήματα, εφαρμογές, βάσεις δεδομένων συμμετέχουν στη διαδικασία backup.
 - Είδος ηλεκτρονικού μέσου αρχειοθέτησης (off-line αποθήκευση) των δεδομένων (π.χ. ταινίες, δίσκοι κ.α.).
 - Ποιό λογισμικό αξιοποιείται για τη δημιουργία των εφεδρικών αντιγράφων.
 - Πως διασφαλίζεται η μακροπρόθεσμη διαθεσιμότητα της τεχνικής ποιότητας του μέσου καταχώρησης;
 - Συχνότητα εφεδρικής αποθήκευσης, αριθμός διαφορετικών εκδόσεων των αντιγράφων ασφαλείας που διατηρούνται.
 - διαδικασίες ελέγχου των εφεδρικών αντιγράφων (δοκιμαστική ανάκτηση των δεδομένων), συχνότητα δοκιμαστικής ανάκτησης δεδομένων.
 - Τοποθεσίες φύλαξης αντιγράφων ασφαλείας.
 - Καθορισμός υπεύθυνου όλης της διαδικασίας backup και restore, που είναι αρμόδιος για καθημερινό έλεγχο της επιτυχής ή όχι λήψης των backups και για έλεγχο της ποιότητας των αντιγράφων ασφαλείας.
 - Ύπαρξη διαδικασίας αποστολής αυτόματου email προς τους υπεύθυνους για την επιτυχή ή όχι ολοκλήρωση της διαδικασίας backup.
 - Ύπαρξη διαδικασιών εναλλακτικής αποθήκευσης, σε περίπτωση που το υπολογιστικό σύστημα δεν λειτουργεί, συμπεριλαμβανομένων των διαδικασιών αποθήκευσης όλων των σχετικών προγραμμάτων και στοιχείων.
 - Ύπαρξη διαδικασίας καταχώρησης και αποθήκευσης των ηλεκτρονικών εγγράφων (συμπεριλαμβανομένης διαδικασίας scanning και microfilm).
 - Ύπαρξη διαδικασίας αρχειοθέτησης και ασφαλούς αποθήκευσης των πάσης φύσεως εγγράφων και πληροφοριών που σχετίζονται με τις επιχειρησιακές διαδικασίες και διαχειρίζονται από τους χρήστες των εφαρμογών, περιλαμβανομένων των αρμοδιοτήτων για τη διαχείρισή τους.

2.6. Τεκμηρίωση Μέτρων Ασφάλειας και Προστασίας των Υποδομών:

- Πολιτική και διαδικασίες μέτρων ασφαλείας για την προστασία των υποδομών πληροφορικής σε επίπεδο δικτυακών συσκευών, εξυπηρετητών, σταθμών εργασίας και εφαρμογών:
 - μέτρα ασφαλείας που λαμβάνονται και υλοποιούνται στις δικτυακές συσκευές (firewall rules, NAT, intrusion detection),
 - εφαρμογές ασφαλείας και προστασίας που χρησιμοποιούνται για τον/τους servers και τους σταθμούς εργασίας:
 - Antivirus, Antispyware, Antispam, Firewalls με όνομα κατασκευστή,

- Αν τα παραπάνω είναι κεντρικές εφαρμογές με clients ανά συσκευή ή εγκαθίστανται σε κάθε συσκευή αυτόνομα,
- Πολιτικές που επιβάλλουν στα συστήματα,
- Ποιος αποφασίζει για την εγκατάσταση των updates σε κάθε σταθμό εργασίας; Ο κάθε χρήστης, ή γίνονται αυτόματα;
- Τομεακές πολιτικές ασφάλειας και λειτουργικότητας (Group/Local Policies) που επιβάλλονται στη χρήση των σταθμών εργασίας.
- Πολιτική χρήσης αφαιρούμενων/φορητών αποθηκευτικών μέσων (εξωτερικοί σκληροί δίσκοι, cd/dvd, usb sticks κ.α.). και κινητών συσκευών (laptops, tablets, smartphones κ.α.).

2.7. Τεκμηρίωση Παρακολούθησης Ορθής Λειτουργίας των Υποδομών:

- Διαδικασία παρακολούθησης και καταγραφής των προβλημάτων που εμφανίζονται στην ορθή λειτουργία του ΠΣ. Περιέχει:
 - Τύπος συστήματος,
 - Τι παρακολουθείται σε αυτό (χρήστες και πρόσβαση, logfiles, monitoring tools κ.α.),
 - Με ποια συχνότητα παρακολουθείται,
 - Ποιος είναι υπεύθυνος για να το παρακολουθεί,
 - Ποια logfiles παρακολουθούνται, πλήρη paths προς τα logfiles,
 - Τι είδους πληροφορία παρακολουθείται στα logfiles,
 - Πού αποθηκεύονται τα logfiles (σε κάθε server, σε κεντρικό σύστημα-αποθετήριο καταγραφής συμβάντων)
 - Ποια είναι τα πιθανά κρίσιμα σφάλματα που μπορεί να εμφανιστούν,
 - Ποιος ενημερώνεται και ενεργεί σε περίπτωση σφάλματος,
 - Πού καταγράφονται και πώς τα περιστατικά (ημερολόγιο συμβάντων).
- Να ανφερθεί αν υπάρχει κεντρικό αποθετήριο καταγραφών (logfiles)
- Ημερολόγιο Συμβάντων για την παρακολούθηση της ορθής λειτουργίας του ΠΣ και των logfiles
- Πολιτική αντιμετώπισης προβλημάτων και αστοχιών υλικού (h/w) και λογισμικού (s/w).

3. Σχέδιο Επιχειρησιακής Συνέχειας και Ανάκτησης από Καταστροφή

Το Σχέδιο Επιχειρησιακής Συνέχειας (**Business Continuity Plan – BCP**) και Ανάκτησης από Καταστροφή (**Disaster Recovery Plan - DRP**) των Πληροφοριακών Συστημάτων (ΣΕΣΑ-ΠΣ) περιλαμβάνει για κάθε πόρο του ΠΣ την παρακάτω πληροφορία:

- Βαθμό βαρύτητας και προτεραιότητας στη λειτουργία της εταιρίας
- Εκτίμηση κινδύνου απώλειας
- Περιγραφή επιπτώσεων στη λειτουργία της εταιρίας από πιθανή απώλεια/δυσλειτουργία
- Εναλλακτικούς τρόπους λειτουργίας της εταιρίας σε περίπτωση μερικής ή ολικής απώλειας
- Διαδικασία αποκατάστασης και θέσης σε επαναλειτουργία σε περίπτωση απώλειας/δυσλειτουργίας, με βάση και το βαθμό βαρύτητας και προτεραιότητας
- Χρόνο αποκατάστασης σε περίπτωση απώλειας/δυσλειτουργίας
- Λίστα υπευθύνων/εμπλεκόμενων σε περίπτωση απώλειας/δυσλειτουργίας, με στοιχεία επικοινωνίας

Ως πόροι του ΠΣ ορίζονται:

- Οι χρήστες (εσωτερικοί και εξωτερικοί),
- Ο εξοπλισμός,
- Οι εφαρμογές,
- Τα κάθε μορφής δεδομένα του σε έντυπη ή ηλεκτρονική μορφή,
- Οι φυσικοί χώροι της εταιρίας όπου είναι εγκατεστημένο.

Συμπληρωματικά (αλλά όχι υποχρεωτικά) στα παραπάνω, προτείνεται η σύνταξη **Πλάνου Αξιολόγησης Κινδύνου** (Risk Assessment) για την καταγραφή και πρόβλεψη των κινδύνων για το ΠΣ, τις επιπτώσεις αυτών στην ορθή λειτουργία των υποδομών και του υ-ΕΟΦ γενικά, και των τρόπων απόκρισης σε κάθε κίνδυνο.

4. Συμβόλαια Συντήρησης και Τεχνικής Υποστήριξης με τρίτες εταιρίες

Η εταιρία πρέπει να διαθέτει συμβόλαια συντήρησης/υποστήριξης των υποδομών (εξοπλισμός, συστήματα και εφαρμογές) με κάθε μία από τις τρίτες εταιρίες που παρέχουν τις ανάλογες υποδομές και υποστηρίζουν την ορθή λειτουργία αυτών. Στα συμβόλαια αυτά πρέπει να υπάρχουν όλοι εκείνοι οι όροι που διασφαλίζουν συμβατικά και τεχνικά την εταιρία.

Πρέπει να επισυναφθούν (εφόσον υπάρχουν) τα Συμβόλαια Συντήρησης και Τεχνικής Υποστήριξης σχετικά με:

- Servers και Σταθμούς Εργασίας
- Έτοιμα Πακέτα Λογισμικού / Εφαρμογές
- Εταιρία που υποστηρίζει τη λειτουργία του ΠΣ

Τα Συμβόλαια πρέπει να περιλαμβάνουν απαραίτητα:

- Επίπεδο Παρεχόμενης Υπηρεσίας (SLA)
- Δήλωση Εμπιστευτικότητας και μη Αποκάλυψης Δεδομένων (NDA)
- Για την περίπτωση της εταιρίας που υποστηρίζει το ΠΣ,
 - πλήρη καταγραφή των παρεχόμενων υπηρεσιών και εργασιών,
 - υποχρέωση συστηματικών περιοδικών ελέγχων ορθής λειτουργίας των συστημάτων και των εφαρμογών του ΠΣ
 - πλήρη περιγραφή της διαδικασίας φυσικής ή/και απομακρυσμένης πρόσβασης και τα δικαιώματα πρόσβασης στους πόρους του ΠΣ της εταιρίας.

5. Πολιτική Ορθής Χρήσης και Δεοντολογίας

Η Πολιτική Ορθής Χρήσης και Δεοντολογίας των Πληροφοριακών Συστημάτων (ΠΟΧΔ-ΠΣ) καθορίζει την ορθή και αποδεκτή χρήση των υποδομών IT της εταιρίας από τους εργαζόμενους και από εξωτερικούς συνεργάτες της. Περιέχει τους κανόνες που εξασφαλίζουν τόσο τους εργαζόμενους όσο και την εταιρία από εσωτερικές ή/και εξωτερικές απειλές στην πληροφοριακή υποδομή της εταιρίας, οι οποίες μπορεί να οδηγήσουν σε:

- κακή χρήση των παρεχόμενων υποδομών,
- μη αποδεκτή ή/και παρατεταμένη διακοπή υπηρεσιών και διαδικασιών,
- μερική ή ολική διακοπή της λειτουργίας της εταιρίας,
- παραβίαση της ασφάλειας των υποδομών,
- εγκατάσταση κακόβουλου λογισμικού,
- μεταβολή, απώλεια ή διαρροή διαβαθμισμένων πληροφοριών ή μη εξουσιοδοτημένη αποκάλυψη διαβαθμισμένων πληροφοριών και πόρων

Σκοπός της ΠΟΧΔ-ΠΣ είναι να ενημερώσει και να ευαισθητοποιήσει τους χρήστες γενικότερα των υποδομών (όπως προσωπικοί υπολογιστές, συστήματα, εφαρμογές, φάκελοι με έντυπο υλικό, φορητά αποθηκευτικά μέσα κ.τ.λ.) ως προς τις ευθύνες τους και τη συνεισφορά τους στην ασφάλεια του ΠΣ και περιλαμβάνει τους απαραίτητους κανόνες ορθής χρήσης που θα πρέπει να ακολουθούνται με σκοπό την ελαχιστοποίηση κινδύνων από αμελή ή κακόβουλη χρήση.

Όλοι οι χρήστες του ΠΣ πρέπει να λαμβάνουν γνώση της ΠΟΧΔ-ΠΣ ενυπόγραφα.

Η ΠΟΧΔ-ΠΣ θα πρέπει να περιέχει τα παρακάτω:

- Ορθή λειτουργία της εταιρίας,
- Ορθή χρήση hardware, software, εφαρμογών, internet, email,
- Ορθή χρήση των passwords,
- Διαδικασία αντιμετώπισης κενών ασφαλείας και περιστατικών που θέτουν σε κίνδυνο το ΠΣ,
- Προστασία Εμπιστευτικότητας,
- Κρίσιμα εταιρικά δεδομένα.

Οι υπάλληλοι θα πρέπει να ενημερώνονται τακτικά (έστω με email) για τις διαδικασίες και τα μέτρα προστασίας του ΠΣ

6. Πιστοποιήσεις από ανεξάρτητους φορείς

Η ύπαρξη πιστοποιήσεων από πιστοποιημένους ανεξάρτητους φορείς δεν είναι απαραίτητη στα πλαίσια της αξιολόγησης της ασφάλειας των ΠΣ της εταιρίας. Αποτελεί ωστόσο μια σαφή ένδειξη/απόδειξη για εξοικείωση της εταιρίας με τήρηση καταγεγραμμένων διαδικασιών σε όλες τις φάσεις της καθημερινής της λειτουργίας.

Συνεπώς, θα πρέπει να απαντηθεί αν η εταιρία έχει λάβει κάποια από τις παρακάτω πιστοποιήσεις;

- **ISO 9001**, Σύστημα Διαχείρισης της Ποιότητας,
- **ISO 14001**, Σύστημα Περιβαλλοντικής Διαχείρισης,
- **ISO 22301**, Σύστημα Διαχείρισης Επιχειρησιακής Συνέχειας,
- **ISO 27001**, Σύστημα Διαχείρισης της Ασφάλειας των Πληροφοριών (είναι το διεθνές πρότυπο για την ασφάλεια πληροφοριών που έχει αυστηρές απαιτήσεις σε όλους τους τομείς που επηρεάζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών και των δεδομένων, από τη φυσική ασφάλεια των εγκαταστάσεων, τη διαχείριση του ανθρωπίνου δυναμικού, τις διαδικασίες λειτουργίας και οργάνωσης, τις σχέσεις με συνεργάτες, πελάτες και τρίτα μέρη, τη συμμόρφωση με νομικές και κανονιστικές απαιτήσεις, μέχρι την ασφάλεια των υποδομών πληροφορικής και επικοινωνιών, τη συνεχή εκπαίδευση και ευαισθητοποίηση του προσωπικού, τον χειρισμό περιστατικών ασφαλείας και τον σχεδιασμό επιχειρησιακής συνέχειας),
- **ISO 20000-1**, Πιστοποίηση Επιχειρήσεων & Τμημάτων Πληροφορικής (είναι το διεθνές πρότυπο απαιτεί την οργάνωση και λειτουργία ενός ολοκληρωμένου συστήματος διεργασιών διαχείρισης, εστιασμένων στην παροχή αποτελεσματικών υπηρεσιών που ικανοποιούν συνεχώς τους πελάτες, εσωτερικούς και εξωτερικούς),
- **ISO 22000**, Σύστημα Διαχείρισης της Ασφάλειας των Τροφίμων,
- **ISO 28000**, Σύστημα Διαχείρισης της Ασφάλειας στην εφοδιαστική αλυσίδα,
- **ISO 31000**, Σύστημα Διαχείρισης Κινδύνου,
- **ISO 13485**, Συστήματος Διαχείρισης Ποιότητας Εταιρειών Παραγωγής και Εμπορίας Ιατροτεχνολογικών Προϊόντων,
- **OHSAS 18001**, Σύστημα για την Ασφάλεια και την Υγεία στους χώρους εργασίας,
- **SA 8000**, Σύστημα Εταιρικής Μέριμνας και Ευθύνης,
- Άλλες πιστοποιήσεις.

Σε περίπτωση ύπαρξης μίας ή παραπάνω πιστοποιήσεων, πρέπει να επισυναφθούν αντίγραφά τους σε ηλεκτρονική μορφή.