ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΝΟΜΟΣ ΗΛΕΙΑΣ
ΔΗΜΟΣ ΗΛΙΔΑΣ

ΑΝΑΡΤΗΤΕΟ ΣΤΗΝ ΙΣΤΟΣΕΛΙΔΑ ΤΟΥ ΔΗΜΟΥ ΚΑΙ ΤΟ ΔΙΑΥΓΕΙΑ

Α Π Ο Σ Π Α Σ Μ Α

Από το πρακτικό τής υπ΄ αριθμ. -9/2023- συνεδρίασης του Δημοτικού Συμβουλίου Ήλιδας.

Αριθμός απόφασης 130/2023

ΘΕΜΑ: «Έγκριση κανονισμού λειτουργίας Πληροφοριακών συστημάτων Δήμου Ήλιδας»

Στην Αμαλιάδα, σήμερα, 27 Ιουνίου 2023, ημέρα Τρίτη και ώρα 20.00΄, συνήλθε σε τακτική δημόσια συνεδρίαση, στο Συνεδριακό Κέντρο τού Πολυλειτουργικού χώρου, το Δημοτικό Συμβούλιο Ήλιδας, κατόπιν της υπ΄ αριθμ. 09/11770/23.06.2023 έγγραφης πρόσκλησης του Προέδρου, η οποία επιδόθηκε νόμιμα και εμπρόθεσμα σε όλα τα μέλη τού Συμβουλίου και τον Δήμαρχο, σύμφωνα με τις διατάξεις τού άρθρου 67 του ν. 3852/10.

Στη συνεδρίαση παραβρέθηκε ο Δήμαρχος κ. Γιάννης Λυμπέρης.

Ο Πρόεδρος διαπίστωσε ότι υπάρχει νόμιμη απαρτία, δεδομένου ότι σε σύνολο «33» μελών βρέθηκαν παρόντα «20», και ονομαστικά οι:

1) Παπαδόπουλος Βασίλειος- Αντιδήμαρχος Δ.Ε Πηνείας
2) Χριστοφόρου Ευάγγελος - Αντιδήμαρχος Καθαριότητας Ηλ/σμού & Πρασίνου
3) Μπούρας Αβραάμ
4) Ζαχαρόπουλος Βασίλειος – Πρόεδρος
5) Κοτσαύτη - Παπαζαφειροπούλου Αλεξάνδρα
6) Γεωργόπουλος Αθανάσιος- Αντιδήμαρχος Αγροτικής, Τουριστικής Ανάπτυξης
7) Παναγιωτάρας Παναγιώτης Αντιδήμαρχος Διοικητικών Υπηρεσιών
8) Μπακέλλας Γεώργιος
9) Παλυβός Χρήστος
10) Χριστοδουλόπουλος Χρήστος [επικεφαλής παράταξης ΗΛΙΔΑ ΝΕΑ ΜΕΡΑ (κλήθηκε κατόπιν της υπ΄αριθμ. 46/22.3.2022 Πράξης κατάθεσης στο ΣτΕ)]
11) Μαρτζάκλη Θεώνη
12) Αναγνωστόπουλος Κωνσταντίνος
13) Ντάνασης Χαράλαμπος
14) Τσεριώνης Κωνσταντίνος
15) Δούλος Παντελής
16) Κολόσακας Άγγελος [επικεφαλής παράταξης ΛΑΪΚΗ ΣΥΣΠΕΙΡΩΣΗ ΗΛΙΔΑΣ]
17) Λοχοβίτης Νικόλαος
18) Κράλλης Δημήτριος [επικεφαλής παράταξης ΗΛΙΔΑ ΝΕΑ ΓΕΝΙΑ ΙΔΕΩΝ]
19) Κράλλης Γεώργιος
20) Χριστόπουλος Ιωάννης - Ανεξάρτητος δ.σ,

Απόντες/Απούσες
(Οι οποίοι/ες δεν προσήλθαν αν και κλήθηκαν νόμιμα)

1. Φουντάς Αθανάσιος, 2.Σταυροπούλου Γιαννούλα, 3. Αστερής Ευγένιος- Αντιδήμαρχος Οικονομικών, 4.Θεοδωρακόπουλος Ιωάννης, 5. Παπαγιαννόπουλος Γεράσιμος, 6. Ανδρουτσόπουλος Ανδρέας, 7. Ευσταθόπουλος Ηλίας, 8. Ανδρικοπούλου-Λαβαζού Κων/να, 09.Αθανασόπουλος Ιωάννης, 10. Παναγόπουλος Χρήστος - Ανεξάρτητος, δ.σ, 11.Παπαδάκος Ανδρέας - Ανεξάρτητος δ.σ. 12.Νικολόπουλος Χρήστος - Ανεξάρτητος δ.σ, 13.Αμπού Χαντμπα Μισέλ

Κατόπιν τούτου, ο Πρόεδρος κήρυξε την έναρξη της συνεδρίασης.

Ο αναπληρωτής δημοτικός υπάλληλος Χρήστος Βούλγαρης τήρησε τα πρακτικά.

Ο Πρόεδρος, ανακοινώνοντας το **27ο** θέμα τής ημερήσιας διάταξης, έθεσε υπόψη των συμβούλων την υπ΄αριθμ. 11744/23.6.2023 εισήγηση του Τμήματος Τεχνολογιών Πληροφορικής & Επικοινωνιών, για Έγκριση κανονισμού λειτουργίας Πληροφοριακών συστημάτων Δήμου Ήλιδας, αναφέροντας τα εξής:

«Όπως γνωρίζετε, ο Δήμος χτυπήθηκε από Ιό τύπου Ransomware, με αποτέλεσμα να τεθεί σχεδόν εξολοκλήρου εκτός λειτουργίας το Πληροφοριακό Σύστημα του. Συγκεκριμένα ο Δήμος δέχτηκε επίθεση από το κακόβουλο λογισμικό την 25/06/2022 και έχει κρυπτογραφηθεί το ψηφιακό αρχείο σε όλους τους Servers του Δήμου που βρίσκονταν σε Domain καθώς επίσης και σε όλους τους ανοιχτούς υπολογιστές στο δίκτυο.

Ο Δήμος Ήλιδας προκειμένου να προβεί στις απαραίτητες εργασίες αποκατάστασης αλλά και να λάβει όλα τα κατάλληλα μέτρα ασφάλειας στο πληροφοριακό σύστημα είχε συνάψει την υπ'αριθμ 19875/26.09.2022 Σύμβαση με τίτλο: ΥΠΗΡΕΣΙΑ ΣΥΜΒΟΥΛΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ με την εταιρία Nisos Advisors. Η εν λόγω σύμβαση παρατάθηκε μέχρι 09/11/2023 μετά την αποδοχή της προσφορά της εταιρίας για Δωρεάν Παροχή Υπηρεσίας Συμβούλου Κυβερνοασφαλείας με την 123/2023 ΑΟΕ.

Στα πλαίσια της παραπάνω σύμβασης η εταιρία έχει καταρτίσει και έχει παραδώσει στον Δήμο Κανονισμό Λειτουργίας Πληροφοριακών Συστημάτων όπου προβλέπονται όλες οι πολίτικές ασφαλείας και οι διαδικασίες που πρέπει να τηρούνται στο Πληροφοριακού Σύστημα του, από όλους τους χρήστες ώστε να εξασφαλίζεται η μέγιστη ασφάλεια δεδομένων και υπηρεσιών.

Παρακαλείτε το σώμα να εγκρίνει τον Κανονισμό Λειτουργίας Πληροφοριακών Συστημάτων Δήμου Ήλιδας»

Ακολούθως ο πρόεδρος κάλεσε τα μέλη να τοποθετηθούν και να ψηφίσουν.

Η παράταξη ΛΑΪΚΗ ΣΥΣΠΕΙΡΩΣΗ ΗΛΙΔΑΣ καταψήφισε το θέμα αιτιολογώντας, ότι δεν μπορεί να προτείνει η εταιρεία τον κανονισμό λειτουργίας που αφορά του δημοτικούς υπαλλήλους, προφανώς για να απαλλάσσεται η ίδια και σε ενδεχόμενη κυβερνο-επίθεση να βρεθούν κατηγορούμενοι πάλι οι εργαζόμενοι.

Το **Δημοτικό Συμβούλιο**, αφού έλαβε υπόψη του:

1. Την εισήγηση της Υπηρεσίας,
2. Τις διατάξεις του ν. 3463/2006, του Δ.Κ.Κ. «Κύρωση του Κώδικα Δήμων και Κοινοτήτων (ΦΕΚ 114/8.6.2006 τεύχος Α΄),

Κατά πλειοψηφία αποφασίζει

Εγκρίνεται ο κανονισμός λειτουργίας Πληροφοριακών συστημάτων Δήμου Ήλιδας, ως εξής:

Γενικός εσωτερικός κανονισμός λειτουργίας των πληροφοριακών συστημάτων του Δήμου

Εισαγωγή

Ο κανονισμός έχει εφαρμογή σε όλο το προσωπικό (χρήστες) και τους εξωτερικούς συνεργάτες του Δήμου, που χρησιμοποιούν τα πληροφοριακά του συστήματα. Όλοι ανεξαιρέτως οι χρήστες οφείλουν να συμμορφώνονται με την υφιστάμενη πολιτική ασφάλειας, τις κατευθύνσεις και οδηγίες του τμήματος πληροφορικής.

Τα πληροφοριακά συστήματα είναι απολύτως απαραίτητα στο προσωπικό του Δήμου, για την εκτέλεση της εργασίας του. Η χρήση των πληροφοριακών συστημάτων ακολουθεί συγκεκριμένους κανόνες με γνώμονα την ασφάλεια της λειτουργίας και των δεδομένων.

Όλοι οι χρήστες, πρέπει να είναι ενημερωμένοι και να συμμορφώνονται με την πολιτική ασφάλειας των πληροφοριακών συστημάτων του Δήμου.

Ορισμοί - συντομογραφίες

Α.Π.Δ.Π.Χ.: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Αρχείο: Ανεξάρτητη λογική οντότητα που αποτελεί συλλογή πληροφοριών σε ηλεκτρονική μορφή.

Διαχειριστής συστήματος: Χρήστης με αυξημένα δικαιώματα επί κάποιου πληροφοριακού συστήματος, στον οποίο έχει ανατεθεί η διαχείριση του συστήματος αυτού.

Ευαίσθητο σύστημα: Οποιοδήποτε σύστημα το οποίο περιέχει εμπιστευτικές πληροφορίες ή παρέχει πρόσβαση σε εμπιστευτικές πληροφορίες.

Κρίσιμο σύστημα: Οποιοδήποτε σύστημα του οποίου η μη διαθεσιμότητα – δυσλειτουργία του, μπορεί να επιφέρει πολύ σοβαρές συνέπειες (οικονομικές, νομικές, λειτουργικές κ.λπ.).

Περιστατικό ασφάλειας: Κάθε συμβάν που δύναται να σχετίζεται με τη μη εφαρμογή της πολιτικής ασφάλειας των πληροφοριακών συστημάτων.

Πληροφορία: Κάθε είδους δεδομένα καθώς και το νόημα που εξάγεται από τη συγκέντρωση, ανάλυση και επεξεργασία των δεδομένων αυτών.

Πληροφοριακά συστήματα: Η/Υ, εξυπηρετητές, εκτυπωτές, μεταγωγείς, δρομολογητές, τα αναχώματα ασφάλειας, λογισμικό, τα συστήματα ανίχνευσης κακόβουλου λογισμικού κ.λπ.

Πληροφοριακός πόρος: Οποιασδήποτε μορφής πληροφορία, αρχεία κ.λπ.

Υπεύθυνος ασφάλειας: Διαχειρίζεται την πολιτική ασφάλειας και επιβλέπει τη σωστή εφαρμογή της.

Χρήστης: Το προσωπικό του Δήμου, συνεργάτες, προμηθευτές και γενικότερα όσοι χρησιμοποιούν τα πληροφοριακά συστήματα του Δήμου.

Γενικές οδηγίες

Η συνεχής και ασφαλής λειτουργία των πληροφοριακών συστημάτων του Δήμου, είναι από τις πρωταρχικές προτεραιότητές του για την εξυπηρέτηση των Δημοτών και παροχή υψηλού επιπέδου ποιότητας υπηρεσιών. Για τους λόγους αυτούς η λειτουργία των πληροφοριακών συστημάτων πρέπει να ακολουθεί το σχετικό νομικό και κανονιστικό πλαίσιο και οι χρήστες να είναι ενήμεροι σχετικά με τα παρακάτω:

Λογική πρόσβαση στα πληροφοριακά συστήματα

Διαδικασία νέου χρήστη:

Υποβολή αιτήματος πρόσβασης

Αξιολόγηση, έγκριση αιτήματος πρόσβασης

Καθορισμός δικαιωμάτων πρόσβασης

Ενημέρωση νέου χρήστη

Προκειμένου να πραγματοποιηθεί χρήση οποιουδήποτε συστήματος, προηγείται ταυτοποίηση του χρήστη από το εν λόγω σύστημα και βάσει της ταυτοποίησης αυτής, του δίνονται τα αντίστοιχα δικαιώματα πρόσβασης - χρήσης.

Η πρόσβαση των χρηστών ελέγχεται με τα ακόλουθα μέτρα:

Τα ονόματα χρηστών (usernames) των χρηστών είναι μοναδικά και άμεσα συσχετισμένα με αυτούς.

Ο κάθε χρήστης έχει εξουσιοδοτημένη πρόσβαση για συγκεκριμένα συστήματα – εφαρμογές.

Ο κάθε χρήστης είναι ενημερωμένος για τα δικαιώματα πρόσβασης και χρήσης που διαθέτει.

Για κάθε ένα σύστημα, διατηρείται αρχείο των χρηστών που διαθέτουν πρόσβαση στα πληροφοριακά συστήματα και τα αντίστοιχα δικαιώματα.

Εφαρμόζεται με τεχνικά μέσα και χωρίς καμία εξαίρεση, η απαίτηση οι κωδικοί πρόσβασης (passwords) να είναι ασφαλείς, σύνθετοι και να αλλάζουν συχνά.

Τα passwords δεν εμφανίζονται σε καμία οθόνη κατά την εισαγωγή τους ούτως ώστε μην να υπάρχει κίνδυνος να υποκλαπούν και να χρησιμοποιηθούν για μη εξουσιοδοτημένη πρόσβαση και χρήση των συστημάτων.

Η σύνδεση ενός χρήστη σε κάποιο σύστημα αναστέλλεται όταν περάσει κάποιο χρονικό διάστημα αδράνειας.

Σε περίπτωση πιθανής διαρροής τα passwords πρέπει να αλλάζουν άμεσα.

Απομακρυσμένη πρόσβαση - Χειρισμός κινητών & λοιπών προσωπικών συσκευών

Η απομακρυσμένη πρόσβαση εφαρμόζεται με τη χρήση τεχνολογιών απομακρυσμένης πρόσβασης και επιτρέπεται μόνο σε εξουσιοδοτημένα πρόσωπα, για τα οποία είναι απόλυτα απαραίτητη, στο πλαίσιο των αρμοδιοτήτων τους.

Ο χρήστης ζητά άδεια, από τον αρμόδιο προϊστάμενο του τμήματος στο οποίο ανήκει, για πρόσβαση από απόσταση. Ο προϊστάμενος του χρήστη ελέγχει το αίτημα και εάν διαπιστώσει ότι πληρούνται οι απαραίτητες προϋποθέσεις, εγκρίνει το αίτημα και το προωθεί (μέσω e-mail) στο τμήμα πληροφορικής. Μετά τις απαραίτητες ρυθμίσεις από το τμήμα πληροφορικής, ο χρήστης αποκτά απομακρυσμένη πρόσβαση στα πληροφοριακά συστήματα .

Εάν γίνεται χρήση προσωπικής συσκευής για υπηρεσιακούς λόγους (π.χ. λήψη e-mail), θα λαμβάνονται τα παρακάτω μέτρα:

Συνεχής εκπαίδευση, ενημέρωση και ευαισθητοποίηση σε θέματα ασφάλειας

Κατάλληλη διαχείριση – διαχωρισμός δεδομένων

Κρυπτογράφηση συσκευών

Χρήση λογισμικού ασφάλειας (antivirus κ.λπ.)

Χρήση κατάλληλων κωδικών ασφάλειας

Σύνδεση μέσω VPN

Συμμόρφωση με την πολιτική ασφάλειας

Στην περίπτωση τηλεργασίας εάν χρησιμοποιηθεί προσωπική συσκευή, θα πρέπει να ακολουθούνται οι παρακάτω βασικές οδηγίες ασφάλειας τηλεργασίας:

Σύνδεση μέσω VPN

Ασφαλής σύνδεση στο Internet (αποφυγή σύνδεσης σε μη ελεγχόμενο – μη ασφαλές δίκτυο)

Αποφυγή αποθήκευσης κωδικών πρόσβασης

Τήρηση μέτρων φυσικής ασφάλειας

Άμεση ενημέρωση σε περίπτωση απώλειας – κλοπής του εξοπλισμού

Συμμόρφωση με την πολιτική ασφάλειας

Αποδεκτή χρήση πληροφοριακών συστημάτων

Για τη χρήση των πληροφοριακών συστημάτων παρέχεται αρχική ενημέρωση στους χρήστες σχετικά με τη διαδικασία πρόσβασης, τη λειτουργία και την ασφάλεια των πληροφοριακών συστημάτων.

Η ενημέρωση των συνεργατών του Δήμου σχετικά με την αποδεκτή χρήση των πληροφοριακών συστημάτων περιλαμβάνει τα παρακάτω:

Οι συνεργάτες ενημερώνονται για την ορθή χρήση των υπηρεσιών στους όρους σύμβασης μεταξύ των δύο μερών. Οι συνεργάτες, μαζί με τους όρους σύμβασης υπογράφουν και το έντυπο εμπιστευτικότητας.

Όλες οι σχετικές απαιτήσεις περί της ασφάλειας πληροφοριών, συμφωνούνται με κάθε προμηθευτή-συνεργάτη που μπορεί να έχει πρόσβαση σε, να επεξεργαστεί, να αποθηκεύσει, να γνωστοποιήσει ή να παράσχει υποδομή πληροφορικής.

Σε περίπτωση που η συνεργασία αφορά προμήθεια προϊόντων, θα επισημαίνεται στις συμβάσεις η ανάγκη για αντιμετώπιση των κινδύνων που ενδεχομένως να προκύψουν από τα νέα προϊόντα. Σε κάθε περίπτωση και ανά τακτά χρονικά διαστήματα, παρακολουθείται και αναθεωρείται η διανομή υπηρεσιών ή προϊόντων των προμηθευτών.

Οι όροι και το έντυπο εμπιστευτικότητας έχουν την αποδοχή του συνεργάτη, προτού ξεκινήσει η συνεργασία και λάβει οποιαδήποτε υπηρεσία. Για οποιαδήποτε αλλαγή στους εν λόγω όρους, υπάρχει έγκαιρη ενημέρωση από τον προϊστάμενο πληροφορικής.

Η υπογεγραμμένη σύμβαση και το έντυπο εμπιστευτικότητας διατηρούνται και από τα δύο μέρη σε πρωτότυπη μορφή.

Τα παρακάτω κριτήρια αποδεκτής χρήσης των πληροφοριακών συστημάτων του Δήμου ισχύουν για όλους ανεξαιρέτως τους χρήστες:

Δεν επιτρέπεται οι χρήστες να εγκαθιστούν, χρησιμοποιούν ή αποθηκεύουν αυτοβούλως μη εξουσιοδοτημένο λογισμικό σε πληροφοριακά συστήματα εκτός από τις περιπτώσεις αλλαγών στο περιβάλλον δοκιμών.

Οι χρήστες δεν πρέπει να διαβάζουν, να τροποποιούν, να διαγράφουν ή να αντιγράφουν αρχεία που ανήκουν σε άλλον χρήστη, χωρίς πρώτα να ζητήσουν άδεια από τον ιδιοκτήτη. Η δυνατότητα ανάγνωσης, τροποποίησης, διαγραφής ή αντιγραφής αρχείων που ανήκουν σε άλλους χρήστες δεν συνεπάγεται την άδεια εκτέλεσης των δραστηριοτήτων αυτών, εκτός και αν ρητά έχει δοθεί τέτοια άδεια.

Οι χρήστες δεν αποκτούν πρόσβαση, να χρησιμοποιούν ή να τροποποιούν πληροφοριακά συστήματα χωρίς εξουσιοδότηση. Επιπλέον, τα συστήματα στα οποία έχουν εξουσιοδότηση χρήσης, θα πρέπει να τα χρησιμοποιούν σύμφωνα με τα δικαιώματα πρόσβασης που τους έχουν αποδοθεί από τον αρμόδιο διαχειριστή συστήματος.

Οι χρήστες μεταχειρίζονται πάσης φύσης λογισμικό σύμφωνα με τους όρους της άδειας χρήσης του λογισμικού. Απαγορεύεται κάθε είδους χρήση, εγκατάσταση ή αντιγραφή λογισμικού που δεν είναι σύμφωνη με την άδεια χρήσης του.

Οι χρήστες δεν πρέπει σκοπίμως να γράφουν, να παράγουν, να μεταγλωττίζουν, να αντιγράφουν, να δημοσιοποιούν, να εκτελούν ή να προσπαθούν να εισάγουν κώδικα υπολογιστών που σχεδιάστηκε για να αυτο-αντιγράφεται, να καταστρέφει ή να παρεμποδίζει την απόδοση οποιουδήποτε αρχείου ή λογισμικού πληροφοριακού συστήματος (με άλλα λόγια, κακόβουλο λογισμικό).

Ρητά απαγορεύεται οποιαδήποτε εσκεμμένη συμπεριφορά που μπορεί να επηρεάσει αρνητικά την ορθή και συνεχή λειτουργία των συστημάτων ή τη δυνατότητα άλλων εξουσιοδοτημένων χρηστών να χρησιμοποιήσουν τα συστήματα.

Δεν επιτρέπεται στους χρήστες ανεξαρτήτως του επιπέδου πρόσβασης που έχουν, να χρησιμοποιούν τα πληροφοριακά συστήματα για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε οποιαδήποτε άλλα συστήματα ή να βλάπτουν, να μεταβάλλουν ή να εμποδίζουν τις λειτουργίες αυτών.

Απαγορεύεται ρητά στους χρήστες να υποκλέπτουν ή με οποιοδήποτε άλλο τρόπο να ανακαλύπτουν συνθηματικά, κρυπτογραφικά κλειδιά ή οποιονδήποτε άλλον μηχανισμό ελέγχου πρόσβασης, ο οποίος θα μπορούσε να τους επιτρέψει μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά συστήματα τρίτων.

Οι χρήστες δεν επιτρέπεται να διενεργούν αυτοβούλως τεχνικούς ελέγχους ασφάλειας στα πληροφοριακά συστήματα. Επιπλέον, ακόμα και στην περίπτωση που εντοπίσουν τυχαία μία αδυναμία ασφάλειας, δεν επιτρέπεται να προσπαθήσουν να εκμεταλλευτούν αυτή την αδυναμία, για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Σε αυτή την περίπτωση, οι χρήστες θα πρέπει να ενημερώσουν άμεσα τον προϊστάμενο πληροφορικής ή τον υπεύθυνο ασφάλειας.

Οι χρήστες είναι υποχρεωμένοι να συμμορφώνονται και να τηρούν τους ορθούς κανόνες χρήσης του διαδικτύου και του ηλεκτρονικού τους ταχυδρομείου.

Οι χρήστες, με το πέρας της εργασίας τους (ή σε περίπτωση πολύωρης απουσίας από τη θέση τους), φροντίζουν να ακολουθούν την πολιτική καθαρής οθόνης του Η/Υ τους (clean screen policy) ώστε να μην παραμένει σε ευαίσθητα δεδομένα ή να περιέχει αρχεία που κάποιος μη εξουσιοδοτημένος θα εκτελούσε με σκοπό την αποκάλυψη στοιχείων. Ο διαχειριστής συστήματος πρέπει να έχει ενεργοποιημένη την προστασία οθόνης (screensaver) από τον εξυπηρετητή.

Στην περίπτωση που διαπιστωθεί μη αποδεκτή χρήση από τους χρήστες, μπορεί να διακοπεί η πρόσβαση στα δεδομένα και στις εφαρμογές, με ενημέρωση του χρήστη για την κρισιμότητα του περιστατικού.

Ασφάλεια δεδομένων - πληροφοριών

Τα θέματα ασφάλειας που προκύπτουν με τη διαρροή πληροφοριών (σε ψηφιακή ή έντυπη μορφή), αφορούν σε απώλεια της εμπιστευτικότητας (με την έννοια της αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένες οντότητες) και της ακεραιότητας των δεδομένων. Οι πληροφορίες πρέπει να προστατεύονται κατάλληλα, ανεξάρτητα από το πού είναι αποθηκευμένες, επεξεργασμένες ή έχουν μεταφερθεί σε άλλα συστήματα.

Ο τρόπος διαβάθμισης, διαχείρισης και αποθήκευσης των πληροφοριών, πρέπει να γίνεται με βάση τη σπουδαιότητα, την αξία, την κρισιμότητα του περιεχομένου της πηγής / μέσου και από την πιθανότητα αποκάλυψης ή τροποποίησης χωρίς εξουσιοδότηση. Την ευθύνη για τον χαρακτηρισμό του επιπέδου διαβάθμισης των πληροφοριών φέρει ο χειριστής τους. Στο πλαίσιο αυτό, καθορίζονται τα παρακάτω επίπεδα διαβάθμισης:

ΑΠΟΡΡΗΤΟ (“Secret”)

ΕΜΠΙΣΤΕΥΤΙΚΟ (“Confidential”)

ΕΣΩΤΕΡΙΚΟ (“Internal”)

ΑΔΙΑΒΑΘΜΗΤΟ (“Public”)

Αρχειοθέτηση των πληροφοριών: Το ψηφιακό αρχείο του Δήμου τηρείται στο σύστημα αρχειοθέτησης και η δομή του έχει εγκριθεί από τον προϊστάμενο πληροφορικής. Η πρόσβαση στο αρχείο θα γίνεται σύμφωνα με τα δικαιώματα που έχουν δοθεί, στη λογική “need to know”. Οι χρήστες είναι υποχρεωμένοι, ανάλογα με τα δικαιώματα πρόσβασης, να καταχωρούν τα έγγραφα σε προκαθορισμένους φακέλους.

Διαχείριση επικοινωνίας μέσω e-mail, skype, drop box, viber κ.λπ.: Οι «απόρρητες» πληροφορίες, που επισυνάπτονται, θα πρέπει να είναι «προστατευμένες» με password το οποίο θα αποστέλλεται με διαφορετικό μέσο ή σε διαφορετική χρονική στιγμή. Οι «εμπιστευτικές» και οι «εσωτερικές» πληροφορίες θα διακινούνται με προσοχή, αλλά χωρίς κάποια προστασία ή επισήμανση.
Πληροφορίες που μεταφέρονται προφορικά (συνομιλίες, τηλέφωνο κ.λπ.): Πρέπει εκ μέρους κάθε εμπλεκόμενου να ακολουθούνται οι διαδικασίες και να τηρείται η «κουλτούρα ασφάλειας», αξιολογώντας την πληροφορία που μεταδίδεται και επιλέγοντας τον ανάλογο χειρισμό.

Ενημέρωση περιστατικών ασφάλειας
Η αναγνώριση ενός περιστατικού ασφάλειας μπορεί να γίνει με τους παρακάτω τρόπους:
Αυτοματοποιημένο μήνυμα (λογισμικό προστασίας ιών, σύστημα ανίχνευσης εισβολών κ.λπ.).
Αναφορά κάποιου χρήστη.
Παρατήρηση «μη κανονικής συμπεριφοράς» στο πληροφοριακό σύστημα.
Άμεσα ενημερώνεται ο προϊστάμενος πληροφορικής, στη συνέχεια ο υπεύθυνος ασφάλειας και εάν απαιτείται η διοίκηση του Δήμου.

Διαδικασίες

1. Αποδεκτής χρήσης
2. Αντιγράφων ασφάλειας
3. Φυσικής πρόσβασης
4. Λογικής πρόσβασης
5. Πρόσβασης διαχειριστών σε κρίσιμα - ευαίσθητα συστήματα
6. Απομακρυσμένης λογικής πρόσβασης
7. Αντιμετώπισης περιστατικών ασφάλειας
8. Αντιμετώπισης κακόβουλου λογισμικού
9. Ασφάλειας δικτύου
10. Διαχείρισης αλλαγών και εγκατάστασης υλικού και λογισμικού
11. Χρήσης κρυπτογραφίας
12. Διαβάθμισης πληροφοριών
13. Ελέγχου ευπαθειών πληροφοριακών συστημάτων
14. Χρήσης κινητών & λοιπών προσωπικών συσκευών

ΠΑΡΑΡΤΗΜΑΤΑ

3.6.1 Διαδικασία αποδεκτής χρήσης

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να καθορίσει τους κανόνες αποδεκτής χρήσης των πληροφοριακών συστημάτων.

Υπεύθυνοι - συμμετέχοντες

Όλοι οι χρήστες φέρουν την ευθύνη για την εφαρμογή της και συμμετέχει ο υπεύθυνος ασφάλειας.

Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο – δοκιμή της διαδικασίας τουλάχιστον κάθε έξι μήνες.

Σχετικά Έντυπα

Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
	Αρχική ενημέρωση χρήστη	Για τη χρήση των πληροφοριακών συστημάτων παρέχεται αρχική ενημέρωση στους χρήστες σχετικά με τη διαδικασία πρόσβασης, τη λειτουργία και την ασφάλεια των πληροφοριακών συστημάτων	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Ενημέρωση συνεργατών	• Οι συνεργάτες ενημερώνονται για την ορθή χρήση των υπηρεσιών στους όρους σύμβασης μεταξύ των δύο μερών. Οι συνεργάτες, μαζί με τους όρους σύμβασης υπογράφουν και το έντυπο εμπιστευτικότητας. • Όλες οι σχετικές απαιτήσεις περί της ασφάλειας πληροφοριών, συμφωνούνται με κάθε προμηθευτή-συνεργάτη που μπορεί να έχει πρόσβαση σε, να επεξεργαστεί, να αποθηκεύσει, να γνωστοποιήσει ή να παράσχει υποδομή πληροφορικής. • Σε περίπτωση που η συνεργασία αφορά προμήθεια προϊόντων, θα επισημαίνεται στις συμβάσεις η ανάγκη για αντιμετώπιση των κινδύνων που ενδεχομένως να προκύψουν από τα νέα προϊόντα. Σε κάθε περίπτωση και ανά τακτά χρονικά διαστήματα, παρακολουθείται και αναθεωρείται η διανομή υπηρεσιών ή προϊόντων των προμηθευτών. • Οι όροι και το έντυπο εμπιστευτικότητας έχουν την αποδοχή του συνεργάτη, προτού ξεκινήσει η συνεργασία και λάβει οποιαδήποτε υπηρεσία. Για οποιαδήποτε αλλαγή στους εν λόγω όρους, υπάρχει έγκαιρη ενημέρωση από τον προϊστάμενο πληροφορικής. • Η υπογεγραμμένη σύμβαση και το έντυπο εμπιστευτικότητας διατηρούνται και από τα δύο μέρη σε πρωτότυπη μορφή.	Συνεργάτες	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Κριτήρια για αποδεκτή χρήση	• Δεν επιτρέπεται οι χρήστες να εγκαθιστούν, χρησιμοποιούν ή αποθηκεύουν αυτοβούλως μη εξουσιοδοτημένο λογισμικό σε	Όλοι οι χρήστες	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	

		πληροφοριακά συστήματα εκτός από τις περιπτώσεις αλλαγών στο περιβάλλον δοκιμών. • Οι χρήστες δεν πρέπει να διαβάζουν, να τροποποιούν, να διαγράφουν ή να αντιγράφουν αρχεία που ανήκουν σε άλλον χρήστη, χωρίς πρώτα να ζητήσουν άδεια από τον ιδιοκτήτη. Η δυνατότητα ανάγνωσης, τροποποίησης, διαγραφής ή αντιγραφής αρχείων που ανήκουν σε άλλους χρήστες δεν συνεπάγεται την άδεια εκτέλεσης των δραστηριοτήτων αυτών, εκτός και αν ρητά έχει δοθεί τέτοια άδεια. • Οι χρήστες δεν αποκτούν πρόσβαση, να χρησιμοποιούν ή να τροποποιούν πληροφοριακά συστήματα χωρίς εξουσιοδότηση. Επιπλέον, τα συστήματα στα οποία έχουν εξουσιοδότηση χρήσης, θα πρέπει να τα χρησιμοποιούν σύμφωνα με τα δικαιώματα πρόσβασης που τους έχουν αποδοθεί από τον αρμόδιο διαχειριστή συστήματος. • Οι χρήστες μεταχειρίζονται πάσης φύσης λογισμικό σύμφωνα με τους όρους της άδειας χρήσης του λογισμικού. Απαγορεύεται κάθε είδους χρήση, εγκατάσταση ή αντιγραφή λογισμικού που δεν είναι σύμφωνη με την άδεια χρήσης του. • Οι χρήστες δεν πρέπει σκοπίμως να γράφουν, να παράγουν, να μεταγλωττίζουν, να αντιγράφουν, να δημοσιοποιούν, να εκτελούν ή να προσπαθούν να εισάγουν κώδικα υπολογιστών που σχεδιάστηκε για να αυτο-αντιγράφεται, να καταστρέφει ή να παρεμποδίζει την απόδοση οποιουδήποτε αρχείου ή λογισμικού πληροφοριακού συστήματος (με άλλα λόγια, κακόβουλο λογισμικό). • Ρητά απαγορεύεται οποιαδήποτε εσκεμμένη συμπεριφορά που μπορεί να επηρεάσει αρνητικά την ορθή και συνεχή λειτουργία των συστημάτων ή τη δυνατότητα άλλων εξουσιοδοτημένων χρηστών να χρησιμοποιήσουν τα συστήματα. • Δεν επιτρέπεται στους χρήστες ανεξαρτήτως του επιπέδου πρόσβασης που έχουν, να χρησιμοποιούν τα πληροφοριακά συστήματα για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε οποιαδήποτε				

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		άλλα συστήματα ή να βλάπτουν, να μεταβάλλουν ή να εμποδίζουν τις λειτουργίες αυτών. • Απαγορεύεται ρητά στους χρήστες να υποκλέπτουν ή με οποιοδήποτε άλλο τρόπο να ανακαλύπτουν συνθηματικά, κρυπτογραφικά κλειδιά ή οποιονδήποτε άλλον μηχανισμό ελέγχου πρόσβασης, ο οποίος θα μπορούσε να τους επιτρέψει μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά συστήματα τρίτων. • Οι χρήστες δεν επιτρέπεται να διενεργούν αυτοβούλως τεχνικούς ελέγχους ασφάλειας στα πληροφοριακά συστήματα. Επιπλέον, ακόμα και στην περίπτωση που εντοπίσουν τυχαία μία αδυναμία ασφάλειας, δεν επιτρέπεται να προσπαθήσουν να εκμεταλλευτούν αυτή την αδυναμία, για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Σε αυτή την περίπτωση, οι χρήστες θα πρέπει να ενημερώσουν άμεσα τον προϊστάμενο πληροφορικής ή τον υπεύθυνο ασφάλειας. • Οι χρήστες είναι υποχρεωμένοι να συμμορφώνονται και να τηρούν τους ορθούς κανόνες χρήσης του διαδικτύου και του ηλεκτρονικού τους ταχυδρομείου. • Οι χρήστες, με το πέρας της εργασίας τους (ή σε περίπτωση πολύωρης απουσίας από τη θέση τους), φροντίζουν να ακολουθούν την πολιτική καθαρής οθόνης του Η/Υ τους (clean screen policy) ώστε να μην παραμένει σε ευαίσθητα δεδομένα ή να περιέχει αρχεία που κάποιος μη εξουσιοδοτημένος θα εκτελούσε με σκοπό την αποκάλυψη στοιχείων. Ο διαχειριστής συστήματος πρέπει να έχει ενεργοποιημένη την προστασία οθόνης (screensaver) από τον εξυπηρετητή. • Στην περίπτωση που διαπιστωθεί μη αποδεκτή χρήση από τους χρήστες, μπορεί να διακοπεί η πρόσβαση στα δεδομένα και στις εφαρμογές, με ενημέρωση του χρήστη για την κρισιμότητα του περιστατικού.				

3.6.2 Διαδικασία αντιγράφων ασφάλειας

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει τις ενέργειες που ακολουθούνται για τη λήψη αντιγράφων ασφάλειας, αφορά όλα τα πληροφοριακά συστήματα και ικανοποιεί τις απαιτήσεις λειτουργίας και ασφάλειας.

2. Υπεύθυνοι - συμμετέχοντες

Ο διαχειριστής συστήματος φέρει την ευθύνη για την εφαρμογή της και συμμετέχουν ο προϊστάμενος πληροφορικής, ο υπεύθυνος ασφάλειας και ο υπεύθυνος προστασίας δεδομένων.

3. Έλεγχος - δοκιμή

Ο διαχειριστής συστήματος φέρει την ευθύνη για τον έλεγχο – δοκιμή της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Σχετικά Έντυπα

5. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
Λήψη αντιγράφων ασφάλειας						
	Καθορισμός αντιγράφων ασφάλειας	Καθορισμός πληροφοριακών συστημάτων για λήψη αντιγράφων ασφάλειας.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Καθορισμός δεδομένων	• Πραγματοποιείται έλεγχος του κανονιστικού πλαισίου ή σχετικής νομοθεσίας (π.χ. απαιτήσεις από Α.Π.Δ.Π.Χ.) προκειμένου να διαπιστωθεί η απαίτηση για τήρηση αντιγράφων ασφάλειας ή ιστορικού του συγκεκριμένου τύπου δεδομένων. • Στην περίπτωση που προκύπτει σχετική απαίτηση, ελέγχεται επιπλέον ο ορισμός από τη νομοθεσία παραμέτρων αναφορικά με την τήρηση. Ενδεικτικά: συχνότητα λήψης αντιγράφων, χρόνος διατήρησης, επίπεδο ασφάλειας κ.λπ. • Ανάλυση των κριτηρίων για επιπτώσεις της απώλειας διαθεσιμότητας των δεδομένων όπως παρακάτω: o Μέγιστος χρόνος έλλειψης: χρονικό διάστημα κατά το οποίο η έλλειψή τους μπορεί να θεωρηθεί αποδεκτή. o Κρισιμότητα: Το μέγεθος των συνεπειών από την έλλειψή τους. o Επιχειρησιακή επίδραση: Εκτίμηση της ενδεχόμενης επίδρασης στην επιχειρησιακή λειτουργία από την έλλειψή τους. • Καθορισμός χρόνου τήρησης δεδομένων. • Τελικός καθορισμός δεδομένων.	Διαχειριστής συστήματος	Υπεύθυνος προστασίας δεδομένων, Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Οργάνωση	• Οργάνωση ημερήσιου online backup.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		• Οργάνωση offline backup, τουλάχιστον 2 φορές την εβδομάδα. • Βασικά στοιχεία οργάνωσης: o Διαθεσιμότητα εναλλακτικού χώρου ασφαλούς αποθήκευσης. o Περιβάλλον λειτουργίας (Test / Επιχειρησιακό / Ανάπτυξης). o Πλάνο Backup: Full, Incremental, Differential κ.λπ. o Τρόπος αποθήκευσης: online, offline.				
	Πρόσβαση	Καθορίζεται το επίπεδο πρόσβασης στα αντίγραφα ασφάλειας.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
Ανάκτηση αντιγράφων ασφάλειας						
	Επιλογή Αντιγράφου Ασφάλειας	Εάν τηρούνται περισσότερα του ενός αντίγραφα ασφάλειας, θα πραγματοποιηθεί επιλογή του πιο πρόσφατου, εφόσον δεν συντρέχουν κάποιο ειδικοί λόγοι για επιλογή άλλου.	Διαχειριστής συστήματος			
	Ανάκτηση Δεδομένων	• Εκτελείται ανάκτηση των δεδομένων σύμφωνα με τις τεχνικές και λειτουργικές απαιτήσεις. • Τα αρχεία τα οποία τελικά ανακτώνται, ελέγχονται για την λειτουργικότητά τους, την ορθότητά τους και τα δικαιώματα πρόσβασης.	Διαχειριστής συστήματος			

3.6.3 Διαδικασία φυσικής πρόσβασης

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να καθορίσει ότι η φυσική πρόσβαση στους χώρους των πληροφοριακών συστημάτων είναι ελεγχόμενη.

2. Υπεύθυνοι - συμμετέχοντες

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για την εφαρμογή της και συμμετέχει ο προϊστάμενος πληροφορικής.

3. Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο – δοκιμή της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Σχετικά Έντυπα

5. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
1.	Γενική περιγραφή	• Επαρκή μέτρα προστασίας και εφαρμογή ελεγχόμενης πρόσβασης στο Computer Room. • Ενημέρωση σε πραγματικό χρόνο για οποιαδήποτε απόπειρα μη εξουσιοδοτημένης πρόσβασης.	Υπεύθυνος ασφάλειας			
	Συστήματα ασφάλειας	• Αυτοματοποιημένο σύστημα ελεγχόμενης πρόσβασης. • Σύστημα συναγερμού. • Σύστημα Κλειστού Κυκλώματος Τηλεόρασης (CCTV).	Υπεύθυνος ασφάλειας			
	Είσοδος – παραμονή επισκεπτών	Για την είσοδο και παραμονή στον χώρο του Computer Room ή στους χώρους των κρίσιμων πληροφοριακών συστημάτων, ισχύουν τα παρακάτω: • Πρέπει σε κάθε περίπτωση να υπάρχει έγκριση από τον προϊστάμενο πληροφορικής. • Καταγράφονται τα στοιχεία των επισκεπτών, η ώρα προσέλευσης και η ώρα αποχώρησής τους. • Οι επισκέπτες ακολουθούν συγκεκριμένες οδηγίες και κανόνες ασφάλειας. • Εργασίες συντήρησης λογισμικού – υλικού, εκτελούνται μόνο από ειδικά εξουσιοδοτημένο προσωπικό.	Διαχειριστής Συστήματος, Προϊστάμενος πληροφορικής	Υπεύθυνος ασφάλειας		

3.6.4 Διαδικασία λογικής πρόσβασης

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει τις ενέργειες, τις τεχνολογίες, τα μέσα και τις διαδικασίες διαχείρισης για την πρόσβαση του κάθε χρήστη στα πληροφοριακά συστήματα και να ελαχιστοποιηθεί ο κίνδυνος της μη εξουσιοδοτημένης πρόσβασης.

2. Υπεύθυνοι - συμμετέχοντες

Ο διαχειριστής συστήματος φέρει την ευθύνη για την εφαρμογή της και συμμετέχουν ο υπεύθυνος ασφάλειας, ο υπεύθυνος προσωπικού και ο προϊστάμενος πληροφορικής.

3. Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο – δοκιμή της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
1.	Περιγραφή πρόσβασης	• Υλοποιούνται λίστες ελέγχου λογικής πρόσβασης, οι οποίες επιτρέπουν την πρόσβαση στα πληροφοριακά συστήματα. • Στην περίπτωση απομακρυσμένης πρόσβασης ακολουθείται η αντίστοιχη διαδικασία.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Προσθήκη νέου χρήστη	• Συμπλήρωση αιτήματος πρόσβασης • Αξιολόγηση και έγκριση αιτήματος πρόσβασης • Απόδοση δικαιωμάτων πρόσβασης • Ενημέρωση χρήστη και ενεργοποίηση δικαιωμάτων πρόσβασης	Χρήστης, Προϊστάμενος χρήστη, Προϊστάμενος πληροφορικής, Διαχειριστής συστήματος			
	Εξουσιοδοτη-μένη πρόσβαση	Προκειμένου να πραγματοποιηθεί χρήση οποιουδήποτε συστήματος, προηγείται ταυτοποίηση του προσώπου από το εν λόγω σύστημα και βάσει της ταυτοποίησης αυτής, του αποδίδονται τα αντίστοιχα προνόμια χρήσης του συστήματος, για τα οποία διαθέτει εξουσιοδότηση.				
	Μέτρα ελέγχου πρόσβασης	• Τα usernames των χρηστών και των χρηστών-συνεργατών είναι μοναδικά και παραπέμπουν στους χρήστες, είναι, δηλαδή άμεσα συσχετισμένα με αυτούς. • Ο κάθε χρήστης διαθέτει εξουσιοδότηση για πρόσβαση που εξυπηρετεί αποκλειστικά τις εφαρμογές στις οποίες είναι εξουσιοδοτημένος. • Ο κάθε χρήστης συνεργάτη διαθέτει εξουσιοδότηση πρόσβασης στα συστήματα που εξυπηρετούν αποκλειστικά τις ανάγκες για τη διεκπεραίωση των καθηκόντων του. • Το επίπεδο των δικαιωμάτων της πρόσβασης που παρέχεται σε κάθε χρήστη συνεργάτη στα συστήματα για τα οποία διαθέτει εξουσιοδότηση	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		είναι το ελάχιστο προκειμένου να καθίσταται ικανός να φέρει εις πέρας τα καθήκοντά του. • Ο κάθε χρήστης συνεργάτη, είναι ενημερωμένος για τα δικαιώματα πρόσβασης και χρήσης που διαθέτει αναφορικά με τα συστήματα. • Για κάθε ένα σύστημα, διατηρείται αρχείο των χρηστών που διαθέτουν πρόσβαση στα πληροφοριακά συστήματα και τα αντίστοιχα δικαιώματα. • Εφαρμογή με τεχνικά μέσα και χωρίς καμία εξαίρεση, της απαίτησης ότι όλα τα passwords να είναι ασφαλή και δύσκολο να “μαντευθούν”. • Τα passwords δεν εμφανίζονται σε καμία οθόνη κατά την εισαγωγή τους ούτως ώστε να μην υπάρχει κίνδυνος να υποκλαπούν και να χρησιμοποιηθούν για μη εξουσιοδοτημένη πρόσβαση και χρήση των συστημάτων. • Εφαρμογή με τεχνικά μέσα και χωρίς καμία εξαίρεση, της απαίτησης όλα τα passwords να αλλάζουν συχνά, όπου αυτό είναι δυνατόν (π.χ. μέσω του Group Policy). • Τα passwords επιδίδονται στους κατόχους τους και αλλάζουν κατά την πρώτη φορά που κάποιος χρήστης αποκτά πρόσβαση σε ένα σύστημα ή εισάγονται στο σύστημα απευθείας από αυτούς με την παρουσία του υπεύθυνου συστήματος. Η διανομή των passwords τηλεφωνικά, απαγορεύεται. Οι νέοι κωδικοί πρόσβασης παραδίδονται στον χρήστη. • Η σύνδεση ενός χρήστη ή χρήστη-συνεργάτη σε κάποιο σύστημα αναστέλλεται όταν περάσει κάποιο χρονικό διάστημα αδράνειας. • Πραγματοποίηση τακτικών δειγματοληπτικών ελέγχων που να αφορούν τον έλεγχο πρόσβασης. Σε περίπτωση ύπαρξης υποψίας διαρροής τα passwords πρέπει να αλλάζουν.				
	Εισαγωγή κωδικών	Μετά την εισαγωγή του ζεύγους username / password, το σύστημα ελέγχει κατά πόσον αντιστοιχούν σε κάποιον έγκυρο χρήστη του.				

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
	πρόσβασης και ασφάλειας	Μόνο σε αυτή την περίπτωση, η διαδικασία συνεχίζεται κανονικά, ως ακολούθως: • Εφόσον πραγματοποιηθεί επιτυχώς η σύνδεση του χρήστη στο σύστημα, το σύστημα ελέγχει κατά πόσον πρόκειται για την πρώτη σύνδεση του χρήστη στο εν λόγω σύστημα ή αν το δοθέν password έχει ξεπεράσει τον χρόνο ζωής του. Και στις 2 περιπτώσεις ο χρήστης είναι υποχρεωμένος να το αλλάξει και προτρέπεται για αυτό. • Αν πρόκειται για την πρώτη σύνδεση του χρήστη ή ο χρόνος ζωής του κωδικού ασφάλειας έχει παρέλθει, η σύνδεση πραγματοποιείται χρησιμοποιώντας τον προσωρινό κωδικό ασφάλειας που του έχει επιδοθεί και είναι υποχρεωμένος να τον αλλάξει. • Σε περίπτωση που ζητηθεί αλλαγή password, ο χρήστης εισάγει πάλι τον κωδικό ασφάλειας που διατηρεί μέχρι εκείνη τη στιγμή και κατόπιν, καλείται να εισάγει τον νέο. Η εισαγωγή πραγματοποιείται δύο φορές, προκειμένου να αποφευχθούν ενδεχόμενα τυπογραφικά λάθη. Το σύστημα πραγματοποιεί έλεγχο εάν ο κωδικός ασφάλειας πληροί όλες τις προδιαγραφές ασφάλειας (πολυπλοκότητα, επαναληψιμότητα κ.λπ.). Ο διαχειριστής συστήματος καλεί τους χρήστες σε αλλαγή των password τους, κάθε τρείς (3) μήνες ή όποτε έχει καθοριστεί στην πολιτική ασφαλείας των Servers (Group Policy). Η διαδικασία συνεχίζεται με τον έλεγχο υπέρβασης του ορίου αποτυχημένων προσπαθειών: • Σε περίπτωση αποτυχημένης προσπάθειας εισαγωγής σε κάποιο σύστημα, το σύστημα διενεργεί έλεγχο κατά πόσον ο αριθμός των αποτυχημένων προσπαθειών έχει ξεπεράσει το ορισμένο όριο των πέντε (5) συνεχόμενων αποτυχημένων προσπαθειών ή του ορίου που έχει καθοριστεί στην πολιτική ασφαλείας των Servers (Group Policy). • Εφόσον το όριο αυτό δεν έχει ξεπεραστεί, ο χρήστης προτρέπεται να εισάγει και πάλι το ζεύγος username / password που του έχουν αποδοθεί.				

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		• Εάν το όριο έχει ξεπεραστεί, τίθενται σε εφαρμογή προληπτικά μέτρα για την ασφάλεια του συστήματος και την αποτροπή ενδεχόμενης μη εξουσιοδοτημένης πρόσβασης. • Η υπέρβαση μέγιστου αριθμού προσπαθειών δεν ισχύει για την πρόσβαση στους servers. Σε περίπτωση υπέρβασης του ορίου αποτυχημένων προσπαθειών ενεργοποιούνται οι προληπτικοί μηχανισμοί προστασίας και τα κατάλληλα μέτρα. Τα προληπτικά μέτρα αφορούν στο κλείδωμα του συστήματος, προκειμένου να μην υπάρχει η δυνατότητα πραγματοποίησης μη εξουσιοδοτημένης πρόσβασης στο σύστημα. Εφόσον πραγματοποιηθούν τα παραπάνω, ο χρήστης πραγματοποιεί χρήση του συστήματος, με βάση τα δικαιώματα χρήστης που του έχουν αποδοθεί.				
	Καταγραφή πρόσβασης	• Κάθε σύνδεση καταγράφεται σε ειδικά αρχεία καταγραφής (log files) για τα οποία δεν υπάρχει δυνατότητα τροποποίησης ή διαγραφής. • Τα ειδικά αρχεία καταγραφής είναι προσβάσιμα μόνο από εξουσιοδοτημένο προσωπικό.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Πρόσβαση από απόσταση	Σύμφωνα με τη διαδικασία απομακρυσμένης πρόσβασης.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Ταυτοποίηση	• Δημιουργία κωδικού πρόσβασης και κωδικού ασφάλειας. • Καθορισμός δικαιωμάτων πρόσβασης.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Τροποποίηση δικαιωμάτων πρόσβασης χρήστη	• Συμπλήρωση αιτήματος πρόσβασης • Αξιολόγηση και έγκριση αιτήματος πρόσβασης • Απόδοση δικαιωμάτων πρόσβασης • Ενημέρωση χρήστη και ενεργοποίηση δικαιωμάτων πρόσβασης	Προϊστάμενος χρήστη, Προϊστάμενος πληροφορικής, Διαχειριστής συστήματος			

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
	Ανάκληση δικαιωμάτων πρόσβασης χρήστη	Η διαδικασία ανάκλησης δικαιωμάτων πρόσβασης χρήστη αφορά στην κανονική και στην επείγουσα ανάκληση των δικαιωμάτων πρόσβασης όπως παρακάτω: • Στην πρώτη περίπτωση, η διαδικασία ξεκινά ύστερα από αίτημα του προϊσταμένου του χρήστη και αφορά στις περιπτώσεις που ένας εργαζόμενος αποχωρεί οριστικά ή αποχωρεί προσωρινά. Το αίτημα αποστέλλεται από τον προϊστάμενο του χρήστη στον προϊστάμενο πληροφορικής σύμφωνα με το σχετικό έντυπο και ακολουθεί η κατάργηση των δικαιωμάτων πρόσβασης. • Στη δεύτερη περίπτωση, ο προϊστάμενος του χρήστη ενημερώνει άμεσα (τηλεφωνικά) τον προϊστάμενο πληροφορικής και ακολουθεί η άμεση κατάργηση των δικαιωμάτων πρόσβασης. Στη συνέχεια, αποστέλλεται το αίτημα σύμφωνα με το σχετικό έντυπο.	Προϊστάμενος χρήστη, Προϊστάμενος πληροφορικής, Διαχειριστής συστήματος			
	Έλεγχος πρόσβασης	Ο έλεγχος της εξουσιοδοτημένης πρόσβασης καλύπτει ολόκληρο τον κύκλο πρόσβασης και χρήσης ενός συστήματος, από τη στιγμή της σύνδεσης ως τη στιγμή της αποσύνδεσης. Τα στοιχεία στα οποία αφορούν οι έλεγχοι που πραγματοποιούνται αναφορικά με τις διαδικασίες της πρόσβασης είναι: • Δικαιώματα πρόσβασης και χρήσης • Αποτελεσματικότητα διαδικασιών • Βαθμός τήρησης διαδικασιών Οι έλεγχοι δικαιωμάτων πρόσβασης και χρήσης πραγματοποιούνται: • Κάθε έξι (6) μήνες. • Εκτάκτως, στην περίπτωση που παρουσιαστεί σχετική ανάγκη (π.χ. εισβολή σε κάποιο σύστημα, παραποίησή του ή οποιοδήποτε σημαντικό περιστατικό ασφάλειας).	Υπεύθυνος ασφάλειας			
	Περιεχόμενο ελέγχου	• Προσεκτική αποτίμηση των αναγκών κάθε συστήματος αναφορικά με τον αριθμό των ατόμων που διαθέτουν δικαιώματα πρόσβασης και χρήσης καθώς και των επιπέδων της πρόσβασης, ούτως ώστε να	Υπεύθυνος ασφάλειας			

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		εξασφαλίζεται η εύρυθμη λειτουργία του συστήματος και η ουσιαστική συνεισφορά του στην επιχειρησιακή λειτουργία. • Ανασκόπηση και καταγραφή των αρμοδιοτήτων του κάθε χρήστη και αντιστοίχισή τους με τα δικαιώματα πρόσβασης και χρήσης που διαθέτει επί των συστημάτων. • Έλεγχος πραγματοποίησης της διαγραφής των δικαιωμάτων πρόσβασης και χρήσης, υπαλλήλων ή συνεργατών που έχουν αποχωρήσει. • Έλεγχος των δικαιωμάτων φυσικής πρόσβασης.				

5. Σχετικά Έντυπα

Πρόσβαση χρήστη
στα πληροφοριακά συστήματα

Οδηγίες

Η αίτηση υποβάλλεται για κάθε μεταβολή που αφορά έναν χρήστη στα πληροφοριακά συστήματα ή κατά την περίπτωση που κάτι τέτοιο κρίνεται αναγκαίο.

Ημερομηνία / /

Ονοματεπώνυμο:

Διεύθυνση / Τμήμα:

Θέση:

Είδος απασχόλησης: ☐ Μόνιμη ☐ Προσωρινή

Ημερομηνία διακοπής πρόσβασης: (εάν η πρόσβαση δεν είναι μόνιμη)

Απαραίτητη Ενέργεια:

- ☐ Δημιουργία νέου χρήστη
- ☐ Τροποποίηση δικαιωμάτων
- ☐ Μεταφορά χρήστη σε άλλο τμήμα
- ☐ Διαγραφή δικαιωμάτων

Προσβάσεις

- ☐ Ηλεκτρονικό ταχυδρομείο
- ☐ Πρόσβαση στο διαδίκτυο
- ☐ Απαιτείται απομακρυσμένη πρόσβαση

Εάν πρόκειται για «Δημιουργία νέου χρήστη» ή «Τροποποίηση δικαιωμάτων» να οριστούν τα δικαιώματα ανά πληροφοριακό σύστημα ως κάτωθι:

Πληροφοριακό Σύστημα	**Read Only**	**Read-Write**	**Read-Write-Delete**
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
Ή δικαιώματα πρόσβασης βάσει ρόλου:			

Παρατηρήσεις / Σχόλια

Εγκρίσεις:

Προϊστάμενος τμήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής
_____	_____	_____

3.6.5 Διαδικασία πρόσβασης διαχειριστών σε κρίσιμα - ευαίσθητα συστήματα

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει τις ενέργειες, τις τεχνολογίες και τα μέσα για την πρόσβαση του κάθε διαχειριστή σε κρίσιμα - ευαίσθητα συστήματα και να ελαχιστοποιηθεί ο κίνδυνος της μη εξουσιοδοτημένης πρόσβασης.

2. Υπεύθυνοι - συμμετέχοντες

Ο διαχειριστής συστήματος φέρει την ευθύνη για την εφαρμογή της και συμμετέχουν ο προϊστάμενος πληροφορικής και ο υπεύθυνος ασφάλειας.

3. Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο – δοκιμή της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
	Περιγραφή πρόσβασης	• Υλοποιούνται λίστες ελέγχου λογικής πρόσβασης, οι οποίες επιτρέπουν την πρόσβαση στα κρίσιμα και ευαίσθητα πληροφοριακά συστήματα. • Στην περίπτωση απομακρυσμένης πρόσβασης ακολουθείται η αντίστοιχη διαδικασία.	Διαχειριστής Συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Εξουσιοδοτημένη πρόσβαση	Προκειμένου να πραγματοποιηθεί χρήση από κάποιον διαχειριστή οποιουδήποτε συστήματος το οποίο έχει χαρακτηριστεί κρίσιμο ή ευαίσθητο, προηγείται ταυτοποίηση του προσώπου από το εν λόγω σύστημα και βάσει της ταυτοποίησης αυτής, του αποδίδονται τα αντίστοιχα προνόμια χρήσης του συστήματος, για τα οποία διαθέτει εξουσιοδότηση.	Διαχειριστής Συστήματος		Προϊστάμενος πληροφορικής	
	Καταγραφή πρόσβασης	• Κάθε σύνδεση καταγράφεται σε ειδικά αρχεία καταγραφής (log files) για τα οποία δεν υπάρχει δυνατότητα τροποποίησης ή διαγραφής. • Τα ειδικά αρχεία καταγραφής είναι προσβάσιμα μόνο από εξουσιοδοτημένο προσωπικό.	Διαχειριστής Συστήματος		Προϊστάμενος πληροφορικής	
	Πρόσβαση από απόσταση	Σύμφωνα με τη διαδικασία απομακρυσμένης πρόσβασης.	Διαχειριστής Συστήματος		Προϊστάμενος πληροφορικής	
	Ταυτοποίηση	• Δημιουργία κωδικού πρόσβασης και κωδικού ασφάλειας. • Καθορισμός δικαιωμάτων πρόσβασης.	Διαχειριστής Συστήματος		Προϊστάμενος πληροφορικής	

5. Σχετικά Έντυπα

Πρόσβαση διαχειριστών
σε κρίσιμα - ευαίσθητα συστήματα

Οδηγίες

Η αίτηση υποβάλλεται για κάθε μεταβολή που αφορά έναν διαχειριστή σε κρίσιμα - ευαίσθητα συστήματα ή κατά την περίπτωση που κάτι τέτοιο κρίνεται αναγκαίο.

Ημερομηνία / /

Ονοματεπώνυμο:	
Διεύθυνση / Τμήμα:	
Θέση:	
Είδος απασχόλησης:	☐ Μόνιμη ☐ Προσωρινή
Ημερομηνία διακοπής πρόσβασης:	(εάν η πρόσβαση δεν είναι μόνιμη)

Απαραίτητη Ενέργεια:

- ☐ Δημιουργία νέου χρήστη
- ☐ Τροποποίηση δικαιωμάτων
- ☐ Μεταφορά χρήστη σε άλλο τμήμα
- ☐ Διαγραφή δικαιωμάτων

Προσβάσεις

- ☐ Ηλεκτρονικό ταχυδρομείο
- ☐ Πρόσβαση στο διαδίκτυο
- ☐ Απαιτείται απομακρυσμένη πρόσβαση

Εάν πρόκειται για «Δημιουργία νέου χρήστη» ή «Τροποποίηση δικαιωμάτων» να οριστούν τα δικαιώματα ανά πληροφοριακό σύστημα ως κάτωθι:

Πληροφοριακό σύστημα	**Read Only**	**Read-Write**	**Read-Write-Delete**
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
Ή δικαιώματα πρόσβασης βάσει ρόλου:			

Παρατηρήσεις / Σχόλια

Εγκρίσεις:

Προϊστάμενος τμήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής
_____	_____	_____

3.6.6 Διαδικασία απομακρυσμένης λογικής πρόσβασης

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει τις ενέργειες, τις τεχνολογίες, τα μέσα και τις διαδικασίες διαχείρισης για την απομακρυσμένη λογική πρόσβαση του κάθε χρήστη στα πληροφοριακά συστήματα και να ελαχιστοποιηθεί ο κίνδυνος της μη εξουσιοδοτημένης πρόσβασης.

2. Υπεύθυνοι - συμμετέχοντες

Ο διαχειριστής συστήματος φέρει την ευθύνη για την εφαρμογή της και συμμετέχουν ο υπεύθυνος ασφάλειας και ο προϊστάμενος πληροφορικής.

3. Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο – δοκιμή της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Σχετικά Έντυπα

5. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
1.	Περιγραφή πρόσβασης	Η πρόσβαση από απόσταση εφαρμόζεται με τη χρήση τεχνολογιών απομακρυσμένης πρόσβασης και επιτρέπεται μόνο σε εξουσιοδοτημένα πρόσωπα, για τα οποία είναι απόλυτα απαραίτητη, στο πλαίσιο των αρμοδιοτήτων τους. Η απομακρυσμένη πρόσβαση στο δίκτυο του φορέα, αν δεν μπορεί να γίνει μέσω Web εφαρμογής (που ελαχιστοποιεί τους κινδύνους προσπέλασης των δεδομένων από εφαρμογή), πραγματοποιείται με τη χρήση Virtual Private Network (VPN) σε συνδυασμό με χρήση μοναδικών προσωπικών ψηφιακών πιστοποιητικών. Η ρύθμιση VPN πραγματοποιείται στο Firewall με απόδοση συγκεκριμένης διεύθυνσης IP, η οποία εκχωρείται δυναμικά από τους μηχανισμούς του δικτύου και είναι μοναδική για κάθε χρήστη. Η κίνηση μεταξύ των χρηστών και του Firewall είναι κρυπτογραφημένη βάσει διεθνώς αποδεκτών προτύπων και αλγορίθμων.	Διαχειριστής Συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Εφαρμογή	• Ο χρήστης ζητά άδεια, από τον αρμόδιο προϊστάμενο του τμήματος στο οποίο ανήκει, για πρόσβαση από απόσταση. • Ο προϊστάμενος του χρήστη ελέγχει το αίτημα και εάν διαπιστώσει ότι πληρούνται οι απαραίτητες προϋποθέσεις, εγκρίνει την άδεια για την έναρξη της διαδικασίας για πρόσβαση από απόσταση και την προωθεί μέσω e-mail στον διαχειριστή συστήματος, με κοινοποίηση στον υπεύθυνο ασφάλειας. Η διαδικασία του αιτήματος δεν εφαρμόζεται μέσω τηλεφωνικής επικοινωνίας. • Ο διαχειριστής συστήματος εκδίδει και εγκαθιστά στον Η/Υ του χρήστη ένα προσωπικό ψηφιακό πιστοποιητικό, εισάγοντας κατά την εγκατάσταση και την προστασία του ιδιωτικού κλειδιού. • Στη συνέχεια, εγκαθιστά πρόγραμμα VPN Client στον Η/Υ του χρήστη - ιδιαίτερη προσοχή πρέπει να δοθεί στον Η/Υ του χρήστη – που	Χρήστης, Προϊστάμενος χρήστη, Προϊστάμενος πληροφορικής, Διαχειριστής συστήματος			

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		είναι κατά βάση φορητός υπολογιστής – να μην είναι ο προσωπικός Η/Υ του υπαλλήλου, να έχει ελεγχθεί με το εγκεκριμένο πρόγραμμα κατά των ιών και να πληροί τις προδιαγραφές ασφάλειας. • Μετά την εγκατάσταση και του προγράμματος-πελάτη (client) στον Η/Υ του χρήστη, ο χρήστης αποκτά πρόσβαση από απόσταση στα συστήματα. • Το κάθε ένα VPN Tunnel το οποίο αρχικοποιείται εγγράφεται στα αρχεία καταγραφής του Firewall.				
	Εξουσιοδοτη-μένη πρόσβαση	Προκειμένου να πραγματοποιηθεί χρήση οποιουδήποτε συστήματος, προηγείται ταυτοποίηση του προσώπου από το εν λόγω σύστημα και βάσει της ταυτοποίησης αυτής, του αποδίδονται τα αντίστοιχα προνόμια χρήσης του συστήματος, για τα οποία διαθέτει εξουσιοδότηση.				
	Καταγραφή πρόσβασης	• Κάθε σύνδεση καταγράφεται σε ειδικά αρχεία καταγραφής (log files) για τα οποία δεν υπάρχει δυνατότητα τροποποίησης ή διαγραφής. • Τα ειδικά αρχεία καταγραφής είναι προσβάσιμα μόνο από εξουσιοδοτημένο προσωπικό.	Διαχειριστής Συστήματος		Προϊστάμενος πληροφορικής	
	Ανάκληση δικαιωμάτων πρόσβασης χρήστη	Η διαδικασία ανάκλησης δικαιωμάτων πρόσβασης χρήστη αφορά στην κανονική και στην επείγουσα ανάκληση των δικαιωμάτων πρόσβασης όπως παρακάτω: • Στην πρώτη περίπτωση, η διαδικασία ξεκινά ύστερα από αίτημα του προϊσταμένου του χρήστη και αφορά στις περιπτώσεις που ένας εργαζόμενος αποχωρεί οριστικά ή αποχωρεί προσωρινά. Το αίτημα αποστέλλεται από τον προϊστάμενο του χρήστη στον προϊστάμενο πληροφορικής με e-mail και ακολουθεί η κατάργηση των δικαιωμάτων πρόσβασης. • Στη δεύτερη περίπτωση, ο προϊστάμενος του χρήστη ενημερώνει άμεσα (τηλεφωνικά) τον προϊστάμενο πληροφορικής και ακολουθεί η	Προϊστάμενος χρήστη, Προϊστάμενος πληροφορικής, Διαχειριστής συστήματος			

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		άμεση κατάργηση των δικαιωμάτων πρόσβασης. Στη συνέχεια, αποστέλλεται το αίτημα με e-mail.				
	Έλεγχος πρόσβασης	Ο έλεγχος της εξουσιοδοτημένης απομακρυσμένης πρόσβασης καλύπτει ολόκληρο τον κύκλο πρόσβασης και χρήσης ενός συστήματος, από τη στιγμή της σύνδεσης ως τη στιγμή της αποσύνδεσης. Τα στοιχεία στα οποία αφορούν οι έλεγχοι που πραγματοποιούνται αναφορικά με τις διαδικασίες της πρόσβασης είναι: • Δικαιώματα πρόσβασης και χρήσης • Αποτελεσματικότητα διαδικασιών • Βαθμός τήρησης διαδικασιών Οι έλεγχοι δικαιωμάτων πρόσβασης και χρήσης πραγματοποιούνται: • Κάθε τρεις (3) μήνες. • Εκτάκτως, στην περίπτωση που παρουσιαστεί σχετική ανάγκη (π.χ. εισβολή σε κάποιο σύστημα, παραποίησή του ή οποιοδήποτε σημαντικό περιστατικό ασφάλειας).	Υπεύθυνος ασφάλειας			

3.6.7 Διαδικασία αντιμετώπισης περιστατικών ασφάλειας

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει τις ενέργειες που ακολουθούνται για την αντιμετώπιση των περιστατικών ασφάλειας που προκύπτουν, τον χειρισμό τους από το υπεύθυνο προσωπικό και την επικοινωνιακή πολιτική που ακολουθείται.

2. Υπεύθυνοι - συμμετέχοντες

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για την εφαρμογή της και συμμετέχει ο προϊστάμενος πληροφορικής.

3. Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο – δοκιμή της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Σχετικά Έντυπα

5. Αναλυτική περιγραφή

Ως σχέδιο αντιμετώπισης περιστατικών ασφάλειας.

3.6.8 Διαδικασία αντιμετώπισης κακόβουλου λογισμικού

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει τα βήματα που ακολουθούνται για την εγκατάσταση και την παραμετροποίηση των απαραίτητων μέτρων προστασίας, προκειμένου να εξασφαλίζεται στον μέγιστο δυνατό βαθμό η προστασία του συνόλου του δικτύου από ιούς ή άλλης μορφής κακόβουλο ή επικίνδυνο λογισμικό.

2. Υπεύθυνοι - συμμετέχοντες

Ο διαχειριστής συστήματος φέρει την ευθύνη για την εφαρμογή της και συμμετέχουν ο υπεύθυνος ασφάλειας και ο προϊστάμενος πληροφορικής.

3. Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο – δοκιμή της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Σχετικά Έντυπα

5. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
1.	Αποτροπή ιών	Χρησιμοποιείται πιστοποιημένο και εγκεκριμένο σύστημα αποτροπής ιών για την προστασία των πληροφοριακών συστημάτων από κακόβουλο λογισμικό. Το λογισμικό έχει εγκατασταθεί σε όλους τους Η/Υ και παρέχει προστασία, τόσο από ιούς, όσο και από κακόβουλο και επικίνδυνο λογισμικό άλλων μορφών. Η διαχείρισή του είναι κεντρική (μέσω Server) και προσφέρει πέραν των άλλων δυνατοτήτων, απαγόρευση λειτουργίας των αφαιρούμενων μέσων αποθήκευσης (USB κτλ.) αλλά και αναστολή απαγόρευσης λειτουργίας τους.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Νέα έκδοση λογισμικού ιών	Ελέγχεται, αν υπάρχει κάποια νέα έκδοση για το λογισμικό προστασίας από ιούς που χρησιμοποιείται. Ο έλεγχος αυτός γίνεται αυτόματα σε καθημερινή βάση ή και σε έκτακτες περιπτώσεις, όταν αυτό καταστεί αναγκαίο. Σε περίπτωση που υπάρχει διαθέσιμη κάποια νέα έκδοση γίνεται η ενημέρωση αυτόματα ή χειροκίνητα οπότε χρειαστεί. Καθορίζεται, αν απαιτούνται κάποιες αλλαγές στις υπάρχουσες default ρυθμίσεις του λογισμικού, ώστε να καλυφθούν με καλύτερο τρόπο οι ανάγκες. Γίνεται η αλλαγή της αντίστοιχης ρύθμισης του λογισμικού προστασίας από ιούς. Ρύθμιση μπορεί να αποτελεί ο αποκλεισμός συγκεκριμένων υπηρεσιών στους χρήστες ή κάποια αλλαγή στον τρόπο απόκρισης του συστήματος σε περίπτωση ανίχνευσης κάποιου ιού. Τέλος, ελέγχεται, αν έχουν πραγματοποιηθεί όλες οι απαιτούμενες αλλαγές στις ρυθμίσεις ή αν κάποιες υπολείπονται.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
	Ενημέρωση λογισμικού ιών	Ελέγχεται, αν υπάρχει κάποια ενημέρωση για νέους ιούς (virus definition) ή κάποιο patch για το λογισμικό προστασίας από ιούς. Ο συγκεκριμένος έλεγχος εκτελείται αυτόματα από το ειδικό λογισμικό σε καθημερινή βάση. Επιπλέον ελέγχεται η εγκυρότητα των στοιχείων ενημέρωσης του λογισμικού προστασίας από ιούς προτού εγκατασταθούν στο σύστημα, αφού υπάρχει η πιθανότητα αλλοίωσης των στοιχείων. Αφού έχουν γίνει οι απαραίτητοι έλεγχοι, εγκαθίστανται οι διαθέσιμες ενημερώσεις ακολουθώντας τα βήματα που καθορίζονται από τον προμηθευτή.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Εγκατάσταση λογισμικού ιών σε νέο Η/Υ	Η διαδικασία προσθήκης νέου Η/Υ ενεργοποιείται με την ανίχνευση κάποιου νέου Η/Υ. Αρχικά γίνεται η εγκατάσταση του ειδικού λογισμικού προστασίας από ιούς στον νέο Η/Υ, ενώ γίνονται και οι κατάλληλες ρυθμίσεις στο ειδικό λογισμικό. Στη συνέχεια ο νέος Η/Υ, προστίθεται στο σύνολο των υπό επίβλεψη συστημάτων του ειδικού λογισμικού προστασίας από ιούς.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Έλεγχος αρχείων συστήματος για κακόβουλο λογισμικό και απαγόρευση χρήσης αφαιρούμενων μέσων αποθήκευσης (USB κ.λπ.)	Ελέγχονται όλα τα αρχεία του συστήματος - συμπεριλαμβανομένου των startup files και των boot records - για ύπαρξη ιών και άλλου είδους κακόβουλο λογισμικό, σε πραγματικό χρόνο αλλά και προγραμματισμένα. Ο έλεγχος πραγματοποιείται σε όλους τους σκληρούς δίσκους, αλλά και στα φορητά αποθηκευτικά μέσα που πιθανώς υπάρχουν και είναι συνδεδεμένα στο σύστημα. Καθορίζεται, αν υπάρχουν πρόσθετα φορητά (αφαιρούμενα) αποθηκευτικά μέσα που πρέπει να ελεγχθούν. Για λόγους αποφυγής προβλημάτων μετάδοσης ιομορφικού λογισμικού, η γενική πολιτική που ακολουθείται είναι η ΑΠΑΓΟΡΕΥΣΗ χρήσης αφαιρούμενων μέσων. Από την παραπάνω πολιτική εξαιρείται το τμήμα πληροφορικής που θα κάνει χρήση συγκεκριμένων Η/Υ στους οποίους θα ελέγχονται αυστηρά όλα τα αφαιρούμενα μέσα που	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		κάποιος χρήστης κατέχει και επιθυμεί να χρησιμοποιήσει δεδομένα από αυτά. Μεγάλη προσοχή δίδεται ΠΡΙΝ την εισαγωγή της συσκευής στον Η/Υ, στο πάτημα και κράτημα του πλήκτρου Shift ώστε να αποτραπεί η αυτόματη εκτέλεση αρχείων. Ο έλεγχος της απαγόρευσης χρήσης των αφαιρούμενων μέσων, θα πραγματοποιείται κατά βάση κεντρικά από το αντιικό πρόγραμμα, το οποίο επιπλέον θα διατηρεί ενημερωμένες βάσεις κατά των ιών.				
	Έλεγχος e-mail	Η εκτέλεση των βημάτων της συγκεκριμένης διαδικασίας ενεργοποιείται με τον εντοπισμό κάποιου νέου εισερχόμενου ή εξερχόμενου μηνύματος ηλεκτρονικής αλληλογραφίας σε κάποιο σταθμό εργασίας ή στον mail server. Αν υπάρχουν επισυναπτόμενα αρχεία στο μήνυμα, ελέγχονται αυτόματα από κατάλληλο λογισμικό.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Αντιμετώπιση ιών	Η διαδικασία αντιμετώπισης ιών ενεργοποιείται από την ανίχνευση κάποιου ιού. Αρχικά, ενημερώνεται το λογισμικό προστασίας από ιούς, ώστε να περιέχει τα πιο πρόσφατα στοιχεία. Γίνεται άμεση ενημέρωση του υπεύθυνου ασφάλειας και του προϊστάμενου πληροφορικής.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Προσδιορι-σμός χαρακτηρι-στικών και επικινδυνό-τητας ιού	Καθορίζονται τα χαρακτηριστικά του ιού, π.χ. το είδος του ιού (virus, worm, trojan horse), καθώς και ο βαθμός επικινδυνότητάς του. Αυτά τα στοιχεία είναι απαραίτητα για την αντιμετώπιση της μόλυνσης.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Εντοπισμός θέσεων μολυσμένων συστημάτων	Εντοπίζονται οι φυσικές θέσεις των Η/Υ που έχουν μολυνθεί. Αναλόγως της έκτασης που έχει λάβει η μόλυνση είναι δυνατό να έχουν μολυνθεί ένα ή περισσότερα υπολογιστικά συστήματα, δικτυακά στοιχεία κ.λπ.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
	Απομόνωση συστημάτων	Στη συνέχεια απομονώνονται τα μολυσμένα συστήματα, ώστε να αντιμετωπιστεί η μόλυνση μεμονωμένα και χωρίς να επηρεάσει τα υπόλοιπα συστήματα. Στο σημείο αυτό, καθορίζεται αν είναι απαραίτητο να διακοπούν κάποιες υπηρεσίες που έχουν επηρεαστεί από τη μόλυνση ή που μπορεί να προκαλέσουν την περαιτέρω εξάπλωσή της.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Διακοπή υπηρεσιών ή/και συνδέσεων	Γίνεται ενημέρωση του υπεύθυνου ασφάλειας και αν κριθεί απαραίτητη η διακοπή υπηρεσιών με έγκρισή του διακόπτονται οι καθορισμένες υπηρεσίες. Οι χρήστες ενημερώνονται εφόσον αυτό κριθεί απαραίτητο για τα προσωρινά μέτρα που έχουν ληφθεί για την αντιμετώπιση της μόλυνσης.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Αφαίρεση μόλυνσης	Εξετάζεται εάν το λογισμικό προστασίας από ιούς διαθέτει τις απαραίτητες πληροφορίες, ώστε να προβεί στην αφαίρεση του ιού από τα μολυσμένα συστήματα χωρίς να επηρεαστεί αρνητικά η λειτουργία τους με κάποιον τρόπο. Αν είναι δυνατή η αυτόματη αφαίρεση του ιού από το λογισμικό προστασίας από ιούς, η μόλυνση αφαιρείται από όλα τα συστήματα. Αν δεν είναι εφικτή η αφαίρεση της μόλυνσης, εξετάζεται εάν υπάρχει η δυνατότητα απομόνωσης ή διαγραφής του αρχείου που περιέχει τον ιό από το λογισμικό προστασίας από ιούς. Και πάλι η συγκεκριμένη ενέργεια επιτρέπεται, μόνο αν αφήνει ανεπηρέαστη τη σωστή λειτουργία των συστημάτων. Αν το αρχείο που περιέχει τον ιό μπορεί να διαγραφεί χωρίς να δημιουργηθεί κάποιο πρόβλημα, το λογισμικό προστασίας από ιούς το διαγράφει. Αν καμία από τις μεθόδους της αφαίρεσης, διαγραφής και απομόνωσης της μόλυνσης δεν μπορεί να εφαρμοστεί σε αυτή την	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		περίπτωση (λόγω π.χ. πιθανής πρόκλησης άλλων προβλημάτων ή μη ικανοποιητικής αντιμετώπισης της μόλυνσης), αναζητούνται πληροφορίες που αφορούν στον συγκεκριμένο ιό. Ακολουθούνται με προσοχή όλα τα βήματα που προτείνονται για την επιτυχή αντιμετώπιση της μόλυνσης. Σε περίπτωση που δεν υπάρχουν όμως πληροφορίες για την αφαίρεση της μόλυνσης, τα μολυσμένα συστήματα μορφοποιούνται εκ νέου (format), καθώς δεν υπάρχει άλλος τρόπος εξάλειψης της μόλυνσης				
	Αποτρεπτικά μέτρα	Ελέγχεται αν είναι δυνατόν να ληφθούν κάποια αποτρεπτικά μέτρα για αποφυγή εκ νέου μόλυνσης από τον ίδιο ή παρόμοιο ιό. Τα μέτρα αυτά μπορεί να περιλαμβάνουν την εκτέλεση κάποιου προγράμματος για θωράκιση του υπολογιστικού συστήματος από τον ιό ή κάποιου patch του προγράμματος προστασίας από ιούς που δεν ήταν διαθέσιμο ή δεν είχε αναπτυχθεί νωρίτερα και αν υπάρχουν εφαρμόζονται με προσοχή.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Επανέλεγχος συστημάτων	Ακολουθεί έλεγχος όλων των υπολογιστικών συστημάτων ή τουλάχιστον των κρίσιμων συστημάτων (συστημάτων που είχαν εντοπιστεί ως μολυσμένα ή είναι πιθανό να μολύνθηκαν στην πορεία) για να επιβεβαιωθεί η επιτυχής αντιμετώπιση της μόλυνσης.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Επαναφορά αρχικών ρυθμίσεων	Όσα συστήματα είχαν απομονωθεί και όσες υπηρεσίες είχαν διακοπεί προσωρινά, προκειμένου να αντιμετωπιστεί η μόλυνση, επαναφέρονται στην αρχική τους κατάσταση. Η επαναφορά των αρχικών ρυθμίσεων γίνεται μόνο όταν έχει αποδειχθεί ότι έχουν εξαλειφθεί όλες οι απειλές και η κανονική λειτουργία των συστημάτων δε θα προκαλέσει κάποιο πρόβλημα. Για τον λόγο αυτό η συγκεκριμένη επαναφορά ενδέχεται να μην πραγματοποιηθεί αμέσως.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Ενημέρωση διαδικασιών	Ο υπεύθυνος ασφάλειας σε συνεργασία με τον προϊστάμενο πληροφορικής τροποποιούν τις διαδικασίες (αν αυτό απαιτείται), προκειμένου να μπορούν παρόμοια περιστατικά να αντιμετωπιστούν πιο αποτελεσματικά στο μέλλον. Επίσης, ελέγχεται, αν χρειάζονται	Υπεύθυνος ασφάλειας		Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		κάποιες αλλαγές στο σύστημα προστασίας από ιούς ή ακόμα και αν είναι απαραίτητη η αντικατάσταση του συστήματος με κάποιο άλλο που μπορεί να καλύψει καλύτερα τις ανάγκες.				

3.6.9 Διαδικασία ασφάλειας δικτύου

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει την εγκατάσταση και την παραμετροποίηση των απαραίτητων μέτρων προστασίας, προκειμένου να εξασφαλίζεται στον μέγιστο δυνατό βαθμό η προστασία του συνόλου του δικτύου.

2. Υπεύθυνοι - συμμετέχοντες

Ο διαχειριστής συστήματος φέρει την ευθύνη για την εφαρμογή της και συμμετέχουν ο υπεύθυνος ασφάλειας και ο προϊστάμενος πληροφορικής.

3. Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο – δοκιμή της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Σχετικά Έντυπα

5. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
1.	Δημιουργία νέου κανόνα	Δημιουργείται ένας νέος κενός κανόνας για το Firewall από τον διαχειριστή συστήματος. Στη συνέχεια καθορίζεται, αν ο νέος κανόνας αποτελεί περιορισμό μόνο για την εισερχόμενη ή την εξερχόμενη κίνηση ή ισχύει και για τους δύο τύπους κίνησης. Αποφασίζεται, αν ο νέος κανόνας θα περιέχει κάποιο έλεγχο θυρών. Αν δηλαδή θα περιορίζεται/ εμποδίζεται κίνηση που προορίζεται για συγκεκριμένες θύρες. Αν θα υπάρχει έλεγχος θυρών, καθορίζονται συγκεκριμένα οι περιορισμοί στις θύρες. Για παράδειγμα μπορεί να εμποδιστεί οποιαδήποτε εισερχόμενη κίνηση κατευθύνεται προς τις θύρες TCP του υπολογιστικού συστήματος. Αποφασίζεται, αν θα γίνει χρήση κάποιου ελέγχου για τη μορφή της διεύθυνσης της πηγής. Αν δηλαδή θα απορρίπτεται κίνηση με συγκεκριμένη τιμή στη διεύθυνση πηγής. Καθορίζονται συγκεκριμένα οι περιορισμοί της διεύθυνσης πηγής. Αποφασίζεται, αν θα γίνει χρήση κάποιου ελέγχου για τη μορφή της διεύθυνσης προορισμού. Αν δηλαδή θα απορρίπτεται κίνηση με συγκεκριμένη τιμή στη διεύθυνση προορισμού. Καθορίζονται συγκεκριμένα οι περιορισμοί της διεύθυνσης προορισμού. Στο σημείο αυτό αποφασίζεται, αν θα γίνει χρήση ελέγχου για το είδος των επιτρεπόμενων πακέτων. Καθορίζονται οι περιορισμοί στο είδος των πακέτων. Θα πρέπει να υπάρχει πάντοτε διαχωρισμός δικτύων, δηλ. διαφορετικά υποδίκτυα για λογικό διαχωρισμό των εφαρμογών και ως εκ τούτου των χρηστών που έχουν πρόσβαση σε αυτές. Αυτό θα τηρείται ως πρακτική, καθότι μέσα από τον καθορισμό των δικαιωμάτων σε επίπεδο εφαρμογών, σε συνδυασμό με τα	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		διαφορετικά υποδίκτυα στα οποία οι χρήστες μπορούν να ανήκουν, διασφαλίζεται ο έλεγχος πρόσβασης στις υπηρεσίες.				
	Εισαγωγή κανόνα και έλεγχος σωστής λειτουργίας Firewall	Ο νέος κανόνας εισάγεται στο σύνολο των κανόνων του συστήματος Firewall. Ελέγχεται η σωστή προσθήκη του κανόνα μέσω της εκτέλεσης ελέγχων που μπορούν να επιβεβαιώσουν την ελεύθερη από σφάλματα λειτουργία του Firewall. Εκτελούνται επίσης οι κατάλληλες ενέργειες σε περίπτωση διαπίστωσης κάποιας παράλειψης.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Επιλογή και διαγραφή κανόνα	Αρχικά επιλέγεται ο προς διαγραφή κανόνας από το σύνολο των διαθέσιμων κανόνων του Firewall. Στη συνέχεια αφαιρείται ο κανόνας που έχει επιλεγεί από το σύνολο των κανόνων του Firewall.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Έλεγχος σωστής λειτουργίας Firewall	Ελέγχεται η σωστή αφαίρεση του κανόνα μέσω της εκτέλεσης ελέγχων που μπορούν να επιβεβαιώσουν την ελεύθερη από σφάλματα λειτουργία του Firewall. Εκτελούνται επίσης οι κατάλληλες ενέργειες σε περίπτωση διαπίστωσης κάποιας παράλειψης.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	

3.6.10 Διαδικασία διαχείρισης αλλαγών και εγκατάστασης υλικού και λογισμικού

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει τις ενέργειες που ακολουθούνται για τη δοκιμή, την αποδοχή και την εγκατάσταση νέου πληροφοριακού εξοπλισμού και τη διαχείριση των αλλαγών που πραγματοποιούνται στα υφιστάμενα πληροφοριακά συστήματα.

Η διαδικασία αφορά όλες τις οργανικές μονάδες και καλύπτει όλο τον πληροφοριακό και επικοινωνιακό εξοπλισμό.

Σημειώνεται ότι η διαδικασία εφαρμόζεται για την εγκατάσταση υλικού ή λογισμικού στα συστήματα εκείνα που έχουν χαρακτηριστεί σαν «Κρίσιμα» ή «Ευαίσθητα». Αντίθετα, δεν εφαρμόζεται για τα συστήματα εκείνα που έχουν χαρακτηριστεί σαν «Μη Κρίσιμα», εκτός εάν προκύπτει ειδικός λόγος.

2. Υπεύθυνοι - συμμετέχοντες

Ο διαχειριστής συστήματος και ο προϊστάμενος πληροφορικής φέρουν την ευθύνη για την εφαρμογή της και συμμετέχει ο υπεύθυνος ασφάλειας.

3. Έλεγχος - δοκιμή

4. Σχετικά Έντυπα

5. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
Προετοιμασία Εγκατάστασης						
1.	Έλεγχος διαθέσιμης τεκμηρίωσης	Αρχικά, ελέγχεται η διαθέσιμη τεκμηρίωση του υπό εγκατάσταση συστήματος. Ο έλεγχος αφορά την πληρότητα και την έκταση της τεκμηρίωσης αναφορικά με την εγκατάσταση, τη διαμόρφωση, τη χρήση και τη συντήρηση του εξοπλισμού. Ιδιαίτερη έμφαση δίνεται: Στα χαρακτηριστικά ασφάλειας του εξοπλισμού. Στις δυνατότητες προστασίας της εμπιστευτικότητας.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Έλεγχος συμμόρφωσης λογισμικού	Στις περισσότερες περιπτώσεις, η εγκατάσταση εξοπλισμού περιλαμβάνει και εγκατάσταση λογισμικού. Στις περιπτώσεις αυτές, ελέγχεται η συμμόρφωση του εν λόγω λογισμικού με καθιερωμένα διεθνή πρότυπα ή διεθνώς διαδεδομένες πρακτικές.	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	
	Αποτίμηση κινδύνου	Πραγματοποιείται αποτίμηση κινδύνου αναφορικά με την ορθή λειτουργία των συστημάτων, που μπορεί να προκύψει από ενδεχόμενη δυσλειτουργία του υπό εγκατάσταση εξοπλισμού. Η αποτίμηση του κινδύνου περιλαμβάνει και την εξέταση των αλληλεξαρτήσεων του υπό εγκατάσταση εξοπλισμού με τα υπάρχοντα τμήματα του εξοπλισμού που βρίσκονται σε λειτουργία.	Υπεύθυνος ασφάλειας			
	Αποδοχή συστήματος	Στο στάδιο αυτό, αποφασίζεται αν ο προς εγκατάσταση εξοπλισμός πληροί – κατ' αρχήν – τις απαραίτητες προϋποθέσεις για την ενσωμάτωσή του στον υφιστάμενο εξοπλισμό. Επιλέγονται κριτήρια που προσομοιάζουν στην καθημερινότητα και αναμένονται αποτελέσματα που εκ των προτέρων είναι γνωστά για δυνατότητα ελέγχου. Επιλέγονται επίσης κριτήρια εκτός επιτρεπόμενων ορίων για διεκπεραίωση της δοκιμής αντοχής της εγκατάστασης. Τα δεδομένα που θα χρησιμοποιηθούν στους ελέγχους	Προϊστάμενος πληροφορικής	Υπεύθυνος ασφάλειας		

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		επιλέγονται με προσοχή και προστατεύονται ως προς την ακεραιότητά τους. Εφόσον η γνωμάτευση είναι θετική, η διαδικασία συνεχίζεται με τον καθορισμό των απαραίτητων δοκιμών που πρέπει να διεξαχθούν. Η θετική γνωμάτευση αποτυπώνεται με την έγκριση του υπεύθυνου ασφάλειας.				
Εγκατάσταση και έλεγχος ορθής λειτουργίας						
	Επιλογή περιβάλ-λοντος εγκατάστα-σης, χρόνου και παραμέτρων υλοποίησης εγκατάστασης - δοκιμών	Ο εξοπλισμός μπορεί κατ' αρχήν να εγκατασταθεί είτε στο περιβάλλον δοκιμής, είτε στο περιβάλλον παραγωγής, εφόσον συντρέχουν ειδικοί λόγοι για αυτό. Εφόσον κριθεί ότι η αρχική εγκατάσταση με σκοπό τη δοκιμή του εξοπλισμού πρέπει να πραγματοποιηθεί απ' ευθείας στο περιβάλλον παραγωγής, πρέπει να γίνει πολύ προσεκτικά η επιλογή του χρόνου κατά τον οποίο θα πραγματοποιηθεί η εγκατάσταση και οι δοκιμές του εξοπλισμού. Σε κάθε περίπτωση, πρέπει να επιλεγεί κατάλληλη χρονική περίοδος, δηλαδή μια περίοδος μη αιχμής. Επιπλέον, θα πρέπει να καθοριστούν όλες οι παράμετροι που ενδεχομένως θα επηρεάσουν την ασφάλεια των πληροφοριακών συστημάτων κατά την εκτέλεση των δοκιμών. Σημειώνεται ότι για την εκτέλεση των δοκιμών θα πρέπει να επιλεγούν δοκιμαστικά δεδομένα, εφόσον αυτό είναι εφικτό, προκειμένου να μην κινδυνεύσει η διασφάλιση των δεδομένων.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Δοκιμαστική εγκατάσταση εξοπλισμού και πραγματοποί-ηση δοκιμών	Εφόσον καθοριστούν όλες οι αναγκαίες παράμετροι, πραγματοποιείται η δοκιμαστική εγκατάσταση του εξοπλισμού, είτε στο περιβάλλον δοκιμών είτε στο περιβάλλον παραγωγής και πραγματοποιούνται οι δοκιμές του προς εγκατάσταση εξοπλισμού, όπως αυτές έχουν οριστεί κατά τη διαδικασία προετοιμασίας της εγκατάστασης.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
	Επικοινωνία με προμηθευτή	Εφόσον κατά την εκτέλεση των δοκιμών του εξοπλισμού παρουσιαστούν προβλήματα, πραγματοποιείται επικοινωνία με τον προμηθευτή για την επίλυσή τους. Για τον σκοπό αυτό, ετοιμάζεται λεπτομερής έκθεση των προβλημάτων η οποία γνωστοποιείται στον προμηθευτή του εξοπλισμού. Ανεξάρτητα από την επικοινωνία με τον προμηθευτή, πραγματοποιείται προσπάθεια για την κατανόηση και επίλυση των δυσλειτουργιών και προβλημάτων και εσωτερικά. Σε κάθε περίπτωση, οι απαιτήσεις ασφάλειας πληροφοριών, συμφωνούνται με τον προμηθευτή και προβλέπονται σαφώς στη συμφωνία, ιδιαίτερα για τις περιπτώσεις που ο προμηθευτής θα έχει πρόσβαση στα πληροφοριακά συστήματα. Επιπλέον, ανά τακτά χρονικά διαστήματα, παρακολουθείται, αναθεωρείται και ελέγχεται η παροχή υπηρεσιών των προμηθευτών, αξιώνοντας την ικανοποίηση των απαιτήσεων ασφάλειας που τέθηκαν αρχικά (ή που εμπλουτίστηκαν αργότερα). Δεν πρέπει ποτέ να διαφεύγει της προσοχής η αναθεώρηση των κινδύνων, προκειμένου με νέα εκτίμηση επικινδυνότητας να τροποποιούνται αναλόγως και οι όροι της συνεργασίας αναφορικά με το επιθυμητό επίπεδο ασφάλειας.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Έγκριση τελικής εγκατάστασης	Εφόσον οι δοκιμές ολοκληρωθούν με επιτυχία ή τα όποια προβλήματα ή δυσλειτουργίες επιλυθούν, η εγκατάσταση του εξοπλισμού εγκρίνεται.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Καθορισμός επιπέδων πρόσβασης στον εξοπλισμό	Μετά την αποδοχή του εξοπλισμού, ο διαχειριστής συστήματος καθορίζει τα επίπεδα πρόσβασης στον εξοπλισμό, δηλώνει δηλαδή ποιοι και υπό ποιες προϋποθέσεις θα έχουν πρόσβαση στον εξοπλισμό. Στη συνέχεια λαμβάνει χώρα η οριστική εγκατάσταση και η διαμόρφωση του εξοπλισμού, στο περιβάλλον παραγωγής. Η εγκατάσταση πραγματοποιείται πάντα σε ώρες μη αιχμής, ώστε να επηρεαστεί στο ελάχιστο η λειτουργία.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
	Ενημέρωση χρηστών	Οι χρήστες ενημερώνονται (αν αυτό είναι απαραίτητο) για την εγκατάσταση του νέου εξοπλισμού και τον τρόπο χειρισμού του.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
Διαχείριση αλλαγών						
	Περιγραφή	Η δημιουργία μιας απαίτησης για τροποποίηση ή αλλαγή, η οποία αναφέρεται ως “Επιχειρησιακή Ανάγκη” πιθανόν να σχετίζεται με: Αλλαγή σε λογισμικό: αλλαγές σε εφαρμογές και λειτουργικά συστήματα που δεν σχετίζονται με το λογισμικό υποδομής (λειτουργικά συστήματα κ.λπ.). Η περίπτωση αυτή αλλαγών δεν περιλαμβάνει τυχόν επείγουσες διορθώσεις. Αλλαγή στον εξοπλισμό (hardware): αλλαγές που σχετίζονται με τον εξοπλισμό της υπάρχουσας υποδομής για την υποστήριξη των εφαρμογών. Επείγουσα αλλαγή (emergency change): αλλαγές που σχετίζονται με προβλήματα που πρέπει να λυθούν άμεσα.				
	Προετοιμασία και υποβολή αιτήματος αλλαγής / εγκατάστασης	Η απαίτηση για αλλαγή τεκμηριώνεται από τον αιτούντα την αλλαγή με τη υποβολή σχετικού αιτήματος. Το αίτημα αυτό περιγράφει αναλυτικά την αλλαγή καθώς και τους λόγους για τους οποίους κρίνεται ότι πρέπει να πραγματοποιηθεί. Επιπλέον, πρέπει να περιγράφει τα συστήματα που επηρεάζονται από την αλλαγή αυτή και τον τρόπο, καθώς και την επίδραση της μη-πραγματοποίησης της αλλαγής. Ενδεικτικά, πιθανοί λόγοι για πραγματοποίηση κάποιας αλλαγής είναι: Ικανοποίηση κάποιας ανάγκης. Ανταπόκριση σε κάποιο τεχνικό πρόβλημα ή πρόληψη πιθανού περιστατικού ασφάλειας. Αναβαθμισμένη έκδοση λογισμικού. Αλλαγή στη νομοθεσία.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		Αύξηση χωρητικότητας συστημάτων.				
	Αρχική αξιολόγηση αιτήματος	Το αίτημα ελέγχεται από τον προϊστάμενο πληροφορικής. Στόχος είναι αφενός να διαπιστωθεί η σκοπιμότητα της αιτούμενης αλλαγής και αφετέρου να διασφαλισθεί ότι το σχετικό αίτημα περιλαμβάνει όλες τις απαιτούμενες πληροφορίες καθώς και ότι το χρονικό διάστημα υλοποίησης που έχει οριστεί είναι αποδεκτό.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Ανάλυση-ενημέρωση για το σχέδιο αλλαγής	Ο διαχειριστής συστήματος ενημερώνει τον προϊστάμενο πληροφορικής σχετικά με τα παρακάτω: Αναγκαιότητα πραγματοποίησης της αλλαγής. Αναλυτικές τεχνικές προδιαγραφές. Καθορισμός δραστηριοτήτων και φάσεων εγκατάστασης. Εκτίμηση ενδεχομένων επιπτώσεων. Ανάλυση των πιθανών επιδράσεων που θα επιφέρει η πιθανή υλοποίηση στο περιβάλλον των κινδύνων ασφάλειας πληροφοριών. Καθορισμός εξουσιοδοτημένου προσωπικού διαχείρισης αλλαγής και υλοποίησης. Χρονοδιάγραμμα υλοποίησης.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Έλεγχος και έγκριση σχεδίου	Ο έλεγχος του σχεδίου είναι αρμοδιότητα του διαχειριστή του συστήματος και του προϊσταμένου πληροφορικής. Πιο αναλυτικά: εξετάζουν την ακρίβεια και την τεχνική αρτιότητα, εκτιμούν τη σπουδαιότητα των αναφερόμενων επιπτώσεων, επιβεβαιώνουν ότι ο υπολογισμός των απαιτούμενων πόρων είναι ακριβής και ελέγχουν την αντίστοιχη διαθεσιμότητα των πόρων και ελέγχουν τον χρονοπρογραμματισμό και επιβεβαιώνουν ότι είναι εφικτός.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
Σχεδιασμός και ανάπτυξη						

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
	Προετοιμασία υλοποίησης	Κατά τη διάρκεια της υλοποίησης ενδέχεται να διακοπούν ορισμένες λειτουργίες ή να παρουσιάσουν προβληματική συμπεριφορά (καθυστερήσεις δικτύου, αδυναμία σύνδεσης κ.λπ.). Η επικοινωνία στους χρήστες τέτοιου είδους πληροφοριών είναι ευθύνη του διαχειριστή συστήματος. Οι χρήστες πρέπει να είναι ενήμεροι σχετικά με: το διάστημα που απαιτείται για την ολοκλήρωση της αλλαγής, τις επιχειρησιακές λειτουργίες που επηρεάζονται, τους χρήστες που πρέπει να ενημερωθούν άμεσα και τις πληροφορίες πρέπει να τους παρασχεθούν, τα συμπτώματα τα οποία ενδέχεται να παρατηρηθούν και εναλλακτικούς τρόπους εργασίας λόγω μη διαθεσιμότητας συγκεκριμένων πόρων κ.λπ.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Ανάπτυξη σχεδίου επαναφοράς	Στην περίπτωση που παρουσιαστούν προβλήματα στο σύστημα κατά τη διάρκεια ή μετά από την ένταξη της σε παραγωγική λειτουργία, θα πρέπει να υπάρχει δυνατότητα επιστροφής στο παλιό σύστημα. Η επαναφορά του συστήματος μπορεί να πραγματοποιηθεί με τους ακόλουθους εναλλακτικούς τρόπους: ανάκληση αλλαγής (αν υπάρχει σχετική δυνατότητα), επαναφορά του συστήματος με χρήση αντιγράφων ασφάλειας που είχαν ληφθεί πριν την πραγματοποίηση της αλλαγής.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Υλοποίηση	Η υλοποίηση πραγματοποιείται σε συμφωνία με τον αναλυτικό σχεδιασμό που έχει γίνει σε συνεργασία με τον διαχειριστή του συστήματος, έχοντας υπόψη ότι αρχικά ενεργοποιείται το περιβάλλον δοκιμών και όχι το παραγωγικό. Σε περίπτωση που συντρέχουν ειδικοί λόγοι για την απευθείας υλοποίηση/εγκατάσταση στο παραγωγικό περιβάλλον, οι αλλαγές	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		πραγματοποιούνται πάντα σε ώρες μη αιχμής, ώστε να ελαχιστοποιείται η επίδραση στη λειτουργία.				
	Εκτέλεση σχεδίου δοκιμών	Θα πρέπει να πραγματοποιηθούν οι κατάλληλοι έλεγχοι που να διασφαλίζουν ότι: δεν θα προκληθούν προβλήματα στη λειτουργία των συστημάτων όλα τα δεδομένα υποβλήθηκαν με το αίτημα (λειτουργικός έλεγχος) η εφαρμογή ανταποκρίνεται σε “δοκιμή” που έχει εκπονηθεί, ειδικά για τον σκοπό αυτό πραγματοποιούνται έλεγχοι που εξασφαλίζουν ότι το σύστημα ικανοποιεί τα κριτήρια αποδοχής Εφόσον διαπιστωθεί η επιτυχής ολοκλήρωση του προκαθορισμένου προγράμματος δοκιμών, δίνεται εντολή από τον διαχειριστή συστήματος για ένταξη σε παραγωγική λειτουργία.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
Υλοποίηση						
	Ενημέρωση εμπλεκόμενων μερών	Η δραστηριότητα αυτή περιλαμβάνει την οριστικοποίηση των πακέτων υλοποίησης και την εξασφάλιση της συμβατότητάς τους σε ό,τι αφορά στις επιπτώσεις, τον χρονοπρογραμματισμό και τους πόρους. Κατά την οριστικοποίηση μπορεί να προκύψει ανάγκη για τροποποιήσεις. Σε αυτή την περίπτωση απαιτείται έγκριση από τον προϊστάμενο πληροφορικής.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Ένταξη σε παραγωγική λειτουργία	Η ένταξη σε παραγωγική λειτουργία πραγματοποιείται σε συμφωνία με τον αναλυτικό σχεδιασμό που έχει γίνει. Η ένταξη διενεργείται από τον εκάστοτε διαχειριστή συστήματος. Σε περίπτωση εμφάνισης προβλημάτων θα πρέπει να ενημερωθούν όσοι επηρεάζονται από την καθυστέρηση και ενδεχομένως να γίνει αναπροσαρμογή του χρονοπρογραμματισμού. Τέλος, στην περίπτωση που παρουσιαστούν προβλήματα στο σύστημα κατά τη διάρκεια ή μετά την ένταξη της αλλαγής, υπάρχει δυνατότητα	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		επιστροφής στο παλιό σύστημα με ενεργοποίηση του σχεδίου επαναφοράς.				
	Ενημέρωση χρηστών	Μετά το πέρας της υλοποίησης εξετάζεται η ενδεχόμενη ανάγκη για ενημέρωση των χρηστών και συνεργατών για τις αλλαγές που πραγματοποιήθηκαν στον εξοπλισμό και τις πιθανές αλλαγές στον τρόπο χειρισμού του. Η ενημέρωση είναι ευθύνη του διαχειριστή συστήματος και οι πληροφορίες που πρέπει να κοινοποιηθούν στους χρήστες σε αυτή την περίπτωση θα πρέπει κατά το ελάχιστο να περιλαμβάνουν τα ακόλουθα: προσδιορισμό της αλλαγής, επιχειρησιακές λειτουργίες που επηρεάζονται και νέες λειτουργίες που είναι διαθέσιμες.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
	Υλοποίηση σχεδίου επαναφοράς και διερεύνηση αιτίων αποτυχίας υλοποίησης	Σε περίπτωση που η ένταξη σε παραγωγική λειτουργία αποτύχει, ενεργοποιείται το κατάλληλο σχέδιο ενώ παράλληλα πραγματοποιείται έλεγχος για τον εντοπισμό των αιτίων που προκάλεσαν την αποτυχία υλοποίησης της αλλαγής στην παραγωγική λειτουργία. Αν κριθεί ότι δύναται να αντιμετωπιστούν τα αίτια αυτά τότε η διαδικασία επιστρέφει στην κανονική ροή. Σε αντίθετη περίπτωση η διαδικασία τερματίζεται.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	
Διαγραφή - απόσυρση υλικού και λογισμικού και αποθηκευτικών μέσων						
	Περιγραφή	Για τη διαχείριση αποθηκευτικών μέσων: εφαρμόζονται ειδικά μέτρα σχετικά με τη χρήση, διακίνηση και την καταστροφή των αποθηκευτικών μέσων, ηλεκτρονικών ή εντύπων, που περιέχουν δεδομένα ή άλλες πληροφορίες που μπορεί να οδηγήσουν σε αποκάλυψη δεδομένων των χρηστών των παρεχόμενων δικτύων ή υπηρεσιών, όπως: Τα αποθηκευτικά μέσα είναι προσβάσιμα ΜΟΝΟ σε εξουσιοδοτημένο προσωπικό.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		Για την καταστροφή των αποθηκευτικών μέσων τηρείται πρωτόκολλο καταστροφής. Το υλικό δεν εξέρχεται από τον χώρο σε καμία περίπτωση. Όποτε απαιτείται καταστροφή του γίνεται εντός του χώρου, μετά από υπογραφή ειδικών συμβάσεων με τις αντίστοιχες εταιρείες διαχείρισης υλικού και λογισμικού.				
	Διαγραφή δεδομένων	Βήματα διαγραφής δεδομένων για Servers και PCs: Αφαίρεση δίσκου από τον server. Αποθήκευση δίσκου στο χρηματοκιβώτιο. Βήματα Διαγραφής Δεδομένων για Storage: Ενημερωτικό e-mail από τον προμηθευτή storage για ελαττωματικό δίσκο. Αίτημα προμήθειας και παραγγελία νέου υλικού. Παραλαβή του καινούργιου δίσκου. Διατήρηση δίσκου για μετέπειτα καταστροφή.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	

3.6.11 Διαδικασία χρήσης κρυπτογραφίας

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει τα βήματα που ακολουθούνται για την εφαρμογή ασφαλών πρωτοκόλλων επικοινωνίας και τη χρήση κρυπτογραφίας.

2. Υπεύθυνοι - συμμετέχοντες

Ο διαχειριστής συστήματος φέρει την ευθύνη για την εφαρμογή της και συμμετέχουν ο υπεύθυνος ασφάλειας και ο προϊστάμενος πληροφορικής.

3. Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Σχετικά Έντυπα

5. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
	Περιγραφή	Τα θέματα ασφάλειας που ανακύπτουν με τη χρησιμοποίηση μη κρυπτογραφικών καναλιών για τη διακίνηση ή διαφύλαξη δεδομένων κρίσιμης σημασίας είναι οι απώλειες της εμπιστευτικότητας και της ακεραιότητας των δεδομένων, η προσποίηση ταυτότητας ενός μη εξουσιοδοτημένου χρήστη καθώς και η άρνηση υπηρεσιών λόγω μιας επίθεσης σε ένα πληροφοριακό σύστημα. Για την ασφαλή μετάδοση δεδομένων πρέπει να έχουν υλοποιηθεί ασφαλή κρυπτογραφικά κανάλια επικοινωνίας χρησιμοποιώντας την τεχνική VPN, η οποία απαιτεί την εμπλοκή ψηφιακού πιστοποιητικού. Ενδεικτικά για τη δημιουργία και μεταφορά των αντιγράφων ασφάλειας από κόμβο σε κόμβο και την πρόσβαση σε κρίσιμα αρχεία και συστήματα απαιτείται η χρήση μηχανισμών κρυπτογράφησης.				
	Χρήση SSL certificates	Χρησιμοποιούνται SSL certificates με συγκεκριμένες ημερομηνίες λήξης, τα οποία παρέχονται ενδεικτικά στις παρακάτω υπηρεσίες: • VPN Service • VM backup Με τον τρόπο αυτό, εξασφαλίζεται και η ασφαλής σύνδεση του client με τον server και η κρυπτογράφηση των δεδομένων που ανταλλάσσονται.	Διαχειριστής συστήματος		Προϊστάμενος πληροφορικής	

3.6.12 Διαδικασία διαβάθμισης πληροφοριών

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει τον τρόπο διαβάθμισης, διαχείρισης και αποθήκευσης των πληροφοριών.

2. Υπεύθυνοι - συμμετέχοντες

Οι χρήστες των πληροφοριακών συστημάτων, ο διαχειριστής συστήματος και ο υπεύθυνος ασφάλειας φέρουν την ευθύνη για την εφαρμογή της και συμμετέχει ο προϊστάμενος πληροφορικής.

3. Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Σχετικά Έντυπα

5. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
1.	Περιγραφή	Τα θέματα ασφάλειας που προκύπτουν με τη διαρροή πληροφοριών (σε ψηφιακή ή έντυπη μορφή), αφορούν σε απώλεια της εμπιστευτικότητας (με την έννοια της αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένες οντότητες) και της ακεραιότητας των δεδομένων. Οι πληροφορίες πρέπει να προστατεύονται κατάλληλα, ανεξάρτητα από το πού είναι αποθηκευμένες, επεξεργασμένες ή έχουν μεταφερθεί σε άλλα συστήματα. Με στόχο την ευαισθητοποίηση του προσωπικού στον χειρισμό πάσης φύσεως πληροφοριών, οι χρήστες θα ενημερώνονται ανά τακτά χρονικά διαστήματα ότι τα μέσα μεταφοράς πληροφόρησης που αφορούν στην εφαρμογή της ασφάλειας είναι (χωρίς το φάσμα να εξαντλείται σε αυτά): • Ηλεκτρονικά έγγραφα • Δεδομένα/πληροφορίες πληροφοριακού συστήματος • Αποθηκευτικά μέσα (backup) • Ηλεκτρονικό ταχυδρομείο (e-mail) • Φόρμες που συμπληρώνονται στο διαδίκτυο (Internet) • Έντυπα έγγραφα • Πληροφορίες που μεταφέρονται προφορικά (συνομιλίες, τηλέφωνο κτλ.) • Λοιπές μορφές αποκάλυψης πληροφοριών				
	Διαβάθμιση πληροφοριών	Ο τρόπος διαβάθμισης, διαχείρισης και αποθήκευσης των πληροφοριών, πρέπει να γίνεται με βάση τη σπουδαιότητα, την αξία, την κρισιμότητα του περιεχομένου της πηγής / μέσου και από την πιθανότητα αποκάλυψης ή τροποποίησης χωρίς εξουσιοδότηση. Την	Όλοι οι χρήστες			

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		ευθύνη για τον χαρακτηρισμό του επιπέδου διαβάθμισης των πληροφοριών φέρει ο χειριστής τους. Στο πλαίσιο αυτό, καθορίζονται τα παρακάτω επίπεδα διαβάθμισης: • ΑΠΟΡΡΗΤΟ (“secret”) • ΕΜΠΙΣΤΕΥΤΙΚΟ (“confidential”) • ΕΣΩΤΕΡΙΚΟ (“internal”) • ΑΔΙΑΒΑΘΜΗΤΟ (“public”)				
	Κατηγοριο-ποίηση Πληροφοριών	ΕΠΙΠΕΔΟ / ΕΙΔΟΣ ΑΠΟΡΡΗΤΟ • Πηγαίος κώδικας • Κωδικοί πρόσβασης • Προσωπικά δεδομένα (όπως ορίζονται κατά GDPR) • Ευαίσθητες πληροφορίες ΕΜΠΙΣΤΕΥΤΙΚΟ • Πολιτικές και διαδικασίες ασφάλειας • Τεχνικές πληροφορίες υποδομής (IPS, routing, σχέδια κ.λπ.) • Vulnerability assessments, penetration tests κ.λπ. • Audit reports, Audit findings και όλη η σχετική επικοινωνία • Alerts / warnings για servers & services • Certificates & σχετικά αρχεία • Οικονομικά στοιχεία • Στοιχεία που αφορούν στο προσωπικό (εξαιρουμένων των όσων θεωρούνται απόρρητα) ΕΣΩΤΕΡΙΚΟ • Πολιτικές και διαδικασίες ποιότητας	Όλοι οι χρήστες			

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
		• Δεδομένα και αρχεία που ανταλλάσσονται μεταξύ των εργαζομένων και δεν χαρακτηρίζονται ως απόρρητα ή εμπιστευτικά • Alerts για missing reports ΑΔΙΑΒΑΘΜΗΤΟ Όλα τα υπόλοιπα που δεν εμπίπτουν σε κάποια από τις ανωτέρω κατηγορίες				
	Αρχειοθέτηση πληροφοριών	Το ψηφιακό αρχείο του Δήμου τηρείται στο σύστημα αρχειοθέτησης και η δομή του έχει εγκριθεί από τον προϊστάμενο πληροφορικής. Η πρόσβαση στο αρχείο θα γίνεται σύμφωνα με τα δικαιώματα που έχουν δοθεί, στη λογική “need to know”. Οι χρήστες είναι υποχρεωμένοι, ανάλογα με τα δικαιώματα πρόσβασης, να καταχωρούν τα έγγραφα σε προκαθορισμένους φακέλους.	Όλοι οι χρήστες			
	Διαχείριση επικοινωνίας μέσω e-mail, skype, drop box, viber κ.λπ.	Οι «απόρρητες» πληροφορίες, που επισυνάπτονται, θα πρέπει να είναι «προστατευμένες» με password το οποίο θα αποστέλλεται με διαφορετικό μέσο ή σε διαφορετική χρονική στιγμή. Οι «εμπιστευτικές» και οι «εσωτερικές» πληροφορίες θα διακινούνται με προσοχή, αλλά χωρίς κάποια προστασία ή επισήμανση.	Όλοι οι χρήστες			
	Πληροφορίες που μεταφέρονται προφορικά (συνομιλίες, τηλέφωνο κ.λπ.)	Πρέπει εκ μέρους κάθε εμπλεκόμενου να ακολουθούνται οι διαδικασίες και να τηρείται η «κουλτούρα ασφάλειας», αξιολογώντας την πληροφορία που μεταδίδεται και επιλέγοντας τον ανάλογο χειρισμό.	Όλοι οι χρήστες			

3.6.13 Διαδικασία ελέγχου ευπαθειών πληροφοριακών συστημάτων

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει τα μέσα και τη μεθοδολογία που χρησιμοποιούνται για τη διενέργεια ελέγχου ευπαθειών στα πληροφοριακά συστήματα.

2. Υπεύθυνοι - συμμετέχοντες

Ο διαχειριστής συστήματος και ο υπεύθυνος ασφάλειας φέρουν την ευθύνη για την εφαρμογή της και συμμετέχει ο προϊστάμενος πληροφορικής.

3. Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Σχετικά Έντυπα

5. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
1.	Περιγραφή	Πρωταρχικό μέτρο ελέγχου των ευπαθειών αποτελεί η επιλογή του κατάλληλου λογισμικού που θα αποκαλύψει τις ευπάθειες και θα προτείνει μέτρα και ενέργειες για την απαλοιφή τους. Οι servers οι οποίοι θα ελέγχονται αναλόγως δικαιώματος πρόσβασης και αναγκαιότητας ελέγχου, πρέπει να καθοριστούν σαφώς ώστε να μην εξαιρεθούν εκ παραδρομής από οποιονδήποτε έλεγχο και να καταγραφούν σε λίστα ελέγχου. Το λογισμικό που θα χρησιμοποιηθεί πρέπει να καλύπτει ευρύ φάσμα απειλών (π.χ. έλεγχο δικτυακών ευπαθειών, web εφαρμογών, configuration εξοπλισμού κ.λπ.). Τα αποτελέσματα μαζί με τις προτάσεις επίλυσης πρέπει να απεικονίζονται σε σωστά δομημένες και αυτοματοποιημένες αναφορές (reports). Οι έλεγχοι θα εκτελούνται ανά τακτά χρονικά διαστήματα.	Διαχειριστής συστήματος, Υπεύθυνος ασφάλειας		Προϊστάμενος πληροφορικής	
	Εκτέλεση ελέγχου ευπαθειών	Πριν την εκτέλεση του ελέγχου ευπαθειών θα ενημερώνεται ο διαχειριστής συστήματος για τις ώρες ελέγχου και έτσι θα υπάρχει η δυνατότητα επισκόπησης των log files που παρήχθησαν κατά τη συγκεκριμένη χρονική περίοδο. Εάν αναπτύσσεται λογισμικό, θα πρέπει να ενημερώνεται επίσης και ο υπεύθυνος ανάπτυξης.	Διαχειριστής συστήματος, Υπεύθυνος ασφάλειας		Προϊστάμενος πληροφορικής	
	Ενημέρωση αποτελεσμά-των ελέγχου ευπαθειών	Με την ολοκλήρωση του ελέγχου ευπαθειών θα ενημερώνονται για τα αποτελέσματα ο προϊστάμενος πληροφορικής και ο υπεύθυνος ασφάλειας.				

3.6.14 Διαδικασία χρήσης κινητών & λοιπών προσωπικών συσκευών

Φορέας:	
Διεύθυνση - Τμήμα:	
email:	
Τηλέφωνο:	

Ιστορικό αναθεωρήσεων

Ημερομηνία	Έκδοση	Ιστορικό αλλαγών ανά έκδοση
	1.0	

Εγκρίσεις

	Ονοματεπώνυμο	Υπογραφή
Ελέγχθηκε - θεωρήθηκε:		

1. Σκοπός – πεδίο εφαρμογής

Η διαδικασία αυτή έχει σκοπό να περιγράψει τις μεθόδους που ακολουθούνται προκειμένου να ελαχιστοποιηθούν ή να μηδενιστούν οι κίνδυνοι που προκύπτουν από τη χρήση κινητών & λοιπών προσωπικών συσκευών. Οι ανάγκες είναι πολλές αλλά και οι “πειρασμοί” είναι μεγάλοι στην εποχή του “mobile computing”, με αποτέλεσμα το να ακολουθηθούν μέτρα και τεχνικές πρόληψης-προστασίας είναι άκρως επιβεβλημένο.

2. Υπεύθυνοι - συμμετέχοντες

Ο διαχειριστής συστήματος και ο υπεύθυνος ασφάλειας φέρουν την ευθύνη για την εφαρμογή της και συμμετέχει ο προϊστάμενος πληροφορικής.

3. Έλεγχος - δοκιμή

Ο υπεύθυνος ασφάλειας φέρει την ευθύνη για τον έλεγχο της διαδικασίας τουλάχιστον κάθε έξι μήνες.

4. Σχετικά Έντυπα

5. Αναλυτική περιγραφή

α/α	Ενέργεια	Περιγραφή	Εφαρμογή	Συμμετοχή	Έγκριση	Παρατηρήσεις
1.	Μέτρα, τεχνικές πρόληψης - προστασίας	• Συνεχής εκπαίδευση, ενημέρωση και ευαισθητοποίηση σε θέματα ασφάλειας • Κατάλληλη διαχείριση – διαχωρισμός δεδομένων • Κρυπτογράφηση συσκευών • Χρήση λογισμικού ασφάλειας (antivirus κλπ.) • Χρήση κατάλληλων κωδικών ασφαλείας • Σύνδεση μέσω VPN • Συμμόρφωση με την πολιτική ασφάλειας	Όλοι οι χρήστες		Υπεύθυνος ασφάλειας	
	Βασικές οδηγίες ασφάλειας τηλεργασίας	• Σύνδεση μέσω VPN • Ασφαλής σύνδεση στο Internet (αποφυγή σύνδεσης σε μη ελεγχόμενο – μη ασφαλές δίκτυο) • Αποφυγή αποθήκευσης κωδικών πρόσβασης • Τήρηση μέτρων φυσικής ασφάλειας • Άμεση ενημέρωση σε περίπτωση απώλειας – κλοπής του εξοπλισμού • Συμμόρφωση με την πολιτική ασφάλειας	Διαχειριστής συστήματος	Υπεύθυνος ασφάλειας	Προϊστάμενος πληροφορικής	

Η απόφαση αυτή πήρε αριθμό – 130- έτους 2023

Ο Πρόεδρος Τα Μέλη

Ακριβές απόσπασμα

Ο Δήμαρχος

Γιάννης Λυμπέρης