ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΝΟΜΟΣ ΠΕΛΛΑΣ
ΔΗΜΟΣ ΑΛΜΩΠΙΑΣ
ΤΜΗΜΑ ΥΠΟΣΤΗΡΙΞΗΣ
ΠΟΛΙΤΙΚΩΝ ΟΡΓΑΝΩΝ
ΓΡΑΦΕΙΟ :ΔΗΜΟΤΙΚΟΥ ΣΥΜΒΟΥΛΙΟΥ

ΑΝΑΡΤΗΤΕΑ

Α Π Ο Σ Π Α Σ Μ Α

ΑΠΟ ΤΟ ΠΡΑΚΤΙΚΟ ΤΗΣ ΑΡΙΘΜ. 16/2024 ΤΑΚΤΙΚΗΣ ΣΥΝΕΔΡΙΑΣΗΣ ΤΟΥ ΔΗΜΟΤΙΚΟΥ ΣΥΜΒΟΥΛΙΟΥ ΑΛΜΩΠΙΑΣ

Αριθμ.Απόφ. 127/2024

ΘΕΜΑ: Έγκριση Κανονισμού Λειτουργίας και Ασφάλειας Πληροφοριακών Συστημάτων Δήμου Αλμωπίας / Ανάλυση Επικινδυνότητας / Πολιτική Ασφάλεια Πληροφοριακών Συστημάτων

Σήμερα **09 Ιουλίου 2024**, ημέρα Τρίτη και ώρα 20.30΄ το Δημοτικό Συμβούλιο Αλμωπίας συνήλθε σε τακτική συνεδρίαση, στο Δημοτικό Κατάστημα Αριδαίας, στην αίθουσα Δημοτικού Συμβουλίου «ΣΥΜΕΩΝ ΣΩΤΗΡΙΑΔΗΣ», σύμφωνα με τις διατάξεις **της παρ. 1 του άρθρου 67 του Ν.3852/2010 όπως αντικαταστάθηκε με το άρθρο 74 του Ν.4555/2018 και το άρθρο 11 του ν.5043/2023**, ύστερα από έγγραφη πρόσκληση του Προέδρου Δ.Σ. με αριθμό 12795/5-7-2024**,** η οποία γνωστοποιήθηκε στον δήμαρχο, στους δημοτικούς συμβούλους και τους Προέδρους Κοινοτήτων με το από 5-7-2024 ηλεκτρονικό μήνυμα.
Διαπιστώθηκε πως υπήρχε νόμιμη απαρτία, δεδομένου ότι σε σύνολο είκοσι πέντε (25) μελών συμμετείχαν τα είκοσι τρία (23) μέλη:

ΠΑΡΟΝΤΑ ΜΕΛΗ ΔΗΜΟΤΙΚΟΥ ΣΥΜΒΟΥΛΙΟΥ

1. Δοβλέτης Ανέστης - Πρόεδρος Δημοτικού Συμβουλίου
2. Θεοδωρίδης Αναστάσιος
3. Ολλανδέζου Όλγα
4. Δερμεντζόγλου Παύλος
5. Κωτσόπουλος Δημήτριος
6. Μήντσης Νικόλαος
7. Χατζηδημητριάδης Γεώργιος
8. Χρυσίδης Παύλος
9. Σαμαράς Θεόδωρος
10. Τζέκος Πέτρος
11. Τσαρκνιάς Πέτρος
12. Σαββίδης Γεώργιος
13. Θεολόγου Ιωάννης
14. Καραμαριάς Αντώνιος
15. Μπάτσης Χρήστος
16. Γιάντσης Δημήτριος
17. Κετικίδης Ιωάννης
18. Σέλκος Ιωάννης
19. Χατζηγιαννίδης Χρήστος
20. Ουργαντζόγλου Ιωσηφίνα
21. Μπίνος Δημήτριος
22. Αβραμίκας Στέφανος
23. Χουρσόγλου Χρήστος

ΑΠΟΝΤΑ ΜΕΛΗ ΔΗΜΟΤΙΚΟΥ ΣΥΜΒΟΥΛΙΟΥ

1. Λαζάρου – Παπαδοπούλου Σταυρούλα
2. Νάνου Πολυξένη

ΠΑΡΟΝΤΕΣ ΠΡΟΕΔΡΟΙ ΚΟΙΝΟΤΗΤΩΝ: επτά (7)

1. Ταρασίδης Δημήτριος – Δ.Κ Αριδαίας
2. Καρυπίδης Κωνσταντίνος – Δ.Κ Αψάλου
3. Διαμαντόπουλος Γαρύφαλλος – Δ.Κ Εξαπλατάνου
4. Ουργαντζόγλου Ευάγγελος – Δ.Κ Θηριόπετρας
5. Γάτσος Εμμανουήλ – Δ.Κ Ίδας
6. Μπίτσκας Δημήτριος – Δ.Κ Ξιφιανής
7. Κοβάτσης Θεολόγος – Δ.Κ. Φούστανης

ΑΠΟΝΤΕΣ ΠΡΟΕΔΡΟΙ ΚΟΙΝΟΤΗΤΩΝ: Είκοσι τρείς (23)
οι οποίοι προσκλήθηκαν νόμιμα σύμφωνα με την παρ.8 του αρθρ. 67 του Ν.3852/2010
Στη συνεδρίαση συμμετείχε ο Δήμαρχος Αλμωπίας, κ. Παρούτογλου Νικόλαος.
Παρούσες στην συνεδρίαση ήταν η Προϊσταμένη του Τμήματος Υποστήριξης Πολιτικών Οργάνων του Δήμου Αλμωπίας, κ. Ίσκου Μαρία και η κ. Θεοδωρίδου Κ. Μεταμόρφη, υπάλληλος Τμήματος Υποστήριξης Πολιτικών Οργάνων, για την τήρηση των πρακτικών.
Παρόντες στη συνεδρίαση ήταν και Πρ/νη Δ/νσης Οικονομικών Υπηρεσιών Δήμου Αλμωπίας, κα Επιγαρίδου Σοφία και ο Πρ/νος τμήματος περιβάλλοντος, καθαριότητας, ανακύκλωσης και συντήρησης πρασίνου, κ. Ιατριδης Γεωργιος.

Ομόφωνα τα μέλη του Δ.Σ. συμφώνησαν να συζητηθεί το μοναδικό θέμα εκτός ημερήσιας διάταξης πριν την συζήτηση των θεμάτων ημερήσιας διάταξης.
Ο κ. Μήντσης Νικόλαος προσήλθε στη συνεδρίαση μετά την ψήφιση του 1ου θέματος εκτός ημερήσιας διάταξης.
Η κα Ουργαντζόγλου Ιωσηφίνα αποχώρησε από τη συνεδρίαση μετά την ψήφιση του 2ου θέματος ημερήσιας διάταξης
Ο κ. Χατζηγιαννίδης Χρήστος αποχώρησε μετά την ψήφιση του 3ου θέματος ημερήσιας διάταξης.
Ο κ. Χουρσόγλου Χρήστος απουσίαζε από την ψήφιση του 1ου θέματος ημερήσιας διάταξης
Απόντες από την ψήφιση του 3ου και 4ου θέματος ημερήσιας διάταξης ήταν οι κ.κ.: Μπάτσης Χρήστος, Θεοδωρίδης Αναστάσιος, Μήντσης Νικόλαος

Ο Πρόεδρος του Δημοτικού Συμβουλίου εισηγούμενος το 4ο θέμα ημερήσιας διάταξης, έθεσε υπόψη των μελών την με αριθ. 142/2024 Απόφαση Δημοτικής Επιτροπής ***Έγκριση Κανονισμού Λειτουργίας και Ασφάλειας Πληροφοριακών Συστημάτων Δήμου Αλμωπίας / Ανάλυση Επικινδυνότητας / Πολιτική Ασφάλεια Πληροφοριακών Συστημάτων.*** σύμφωνα με την οποία η Δημοτική Επιτροπή κατόπιν της με αριθ. 10686/03-06-2024 εισήγησης της Προϊστάμενης του Τμήματος Προγραμματισμού Οργάνωσης και Πληροφορικής του Δήμου Αλμωπίας, εγκρίνει και εισηγείται στο Δημοτικό Συμβούλιο το προτεινόμενο σχέδιο του **Κανονισμού Λειτουργίας και Ασφάλειας των Πληροφοριακών Συστημάτων του Δήμου Αλμωπίας / Ανάλυση Επικινδυνότητας / Πολιτική Ασφάλεια Πληροφοριακών Συστημάτων.**
Ακολούθησε αναλυτική διαλογική συζήτηση των μελών με προτάσεις και ερωτήσεις, όπως καταγράφηκε στα μαγνητοφωνημένα πρακτικά της με αριθ. 16/2024 συνεδρίασης Δ.Σ.
Κατόπιν ο Πρόεδρος του Δ.Σ. κάλεσε τα μέλη να ψηφίσουν το θέμα όπως κατατέθηκε με την αριθ. 142/2024 Απόφαση Δημοτικής Επιτροπής.
Το Δ.Σ. αφού άκουσε την εισήγηση του Προέδρου της και έλαβε υπόψη:

- Τα άρθρα 72, 74, 74Α, και 75 του Ν.3852/2010, όπως τροποποιήθηκε και ισχύει.
- Το άρθρο 74Α παρ.1 ν.3852/10, όπως προστέθηκε από το άρθρο 9 του ν.5056/23
- Τις διατάξεις του Ν.4735/2020
- Τις διατάξεις του Ν.4722/2020
- Τις διατάξεις του Ν.5013/2023
- Το άρθρο 30 του Ν.5056/2023
- Το Έντυπο 1. Ανάλυση Επικινδυνότητας

- Το Έντυπο 2. Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων
- Την αρ. 142/2024 Απόφαση Δημοτικής Επιτροπής.
- την διαλογική συζήτηση των μελών όπως καταγράφηκε στα μαγνητοφωνημένα πρακτικά της ν.16/2024 συνεδρίασης

Αποφασίζει ομόφωνα

Εγκρίνει τον **Κανονισμό Λειτουργίας και Ασφάλειας των Πληροφοριακών Συστημάτων του Δήμου Αλμωπίας / Ανάλυση Επικινδυνότητας / Πολιτική Ασφάλεια Πληροφοριακών Συστημάτων**, όπως διαβιβάστηκε με την αριθ. 142/2024 Απόφαση Δημοτικής Επιτροπής, ήτοι :

ΔΗΜΟΣ ΑΛΜΩΠΙΑΣ

ΤΜΗΜΑ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥΟΡΓΑΝΩΣΗΣ & ΠΛΗΡΟΦΟΡΙΚΗΣ ΔΗΜΟΥ ΑΛΜΩΠΙΑΣ
ΓΡΑΦΕΙΟ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΕΠΙΚΟΙΝΩΝΙΩΝ

ΚΑΝΟΝΙΣΜΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΔΗΜΟΥ ΑΛΜΩΠΙΑΣ

ΕΝΤΥΠΟ 1
ΑΝΑΛΥΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Αριδαία, 8 Απριλίου 2024

Περιεχόμενα

ΕΝΤΥΠΟ 1
Ανάλυση Επικινδυνότητας(Risk Analysis)

1 Εισαγωγή

Σκοπός του παρόντος Εντύπου 1 είναι αρχικά η αποτύπωση των Πληροφοριακών Συστημάτων του Δήμου Αλμωπίας, ακολούθως γίνεται ανάλυση των παρακάτω θεμάτων ασφάλειας:

- Ανάλυση Επικινδυνότητας(Risk Analysis)

Σε διαφορετικό έντυπο 2 σημειώνεται η περιγραφόμενη Πολιτική Ασφαλείας και οι προτεινόμενες δράσεις. Ο «**ΚΑΝΟΝΙΣΜΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΤΟΥ ΔΗΜΟΥ ΑΛΜΩΠΙΑΣ ΕΝΤΥΠΟ 2 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ & ΔΙΚΤΥΩΝ ΥΠΗΡΕΣΙΩΝ ΔΗΜΟΥ ΑΛΜΩΠΙΑΣ** περιορίζεται κυρίως σε κινδύνους και θέματα που σχετίζονται με τα πληροφοριακά συστήματα του Δήμου Αλμωπίας.

Ακολουθεί η περιγραφή της υφιστάμενης κατάστασης των πληροφοριακών συστημάτων του Δήμου Αλμωπίας

Γενικά:

Ο Δήμος Αλμωπίας είναι ΟΤΑ και κτηριακά χωρίζεται στο:

1. Κεντρικό Δημαρχείο - Δημοτολόγιο – Ληξιαρχείο Αριδαία
2. Πολεοδομία Αριδαία
3. ΚΕΠ Αριδαίας
4. Βοήθεια στο Σπίτι – Παράρτημα Εφορίας (Παλαιό Δημαρχείο Αριδαίας)
5. Εργοτάξιο Αριδαία
6. Δημοτική Ενότητα Εξαπλατάνου – Κέντρο Κοινότητας στον Εξαπλάτανο
7. ΚΕΠ Εξαπλατάνου

Σε κάθε κτήριο ξεχωριστά υπάρχει εξοπλισμός Σύζευξης με τον οποίον αφενός συνδέονται στο διαδίκτυο τα τερματικά του κάθε κτηρίου και αφετέρου επιτυγχάνεται και η εσωτερική διασύνδεση σε επίπεδο τοπικού δικτύου κάθε κτηρίου. Η φυσική ενοποίηση σε τόσα απομακρυσμένα σημεία δεν είναι εύκολη, η λογική τους ωστόσο ενοποίηση έχει επιτευχθεί (αν και οι ταχύτητες σύνδεσης δεν είναι σε όλα τα κτήρια ικανοποιητικές), μέσω της άρσης περιμετρικής ασφάλειας που έχουμε αιτηθεί. Ουσιαστικά επιτεύχθηκε η λογική ενοποίηση που επέτρεψε την κεντρική μηχανογραφική διαχείριση με τα παρακάτω ενδεικτικά οφέλη:

Οποιοδήποτε τερματικό κάθε κτηρίου έχει πρόσβαση στο FILESERVER(NAS) που βρίσκεται στο κεντρικό Δημαρχείο και να ανταλλάσει αρχεία εσωτερικά ως ένα υπηρεσιακό δίκτυο WANμέσω Σύζευξις

Οποιοδήποτε τερματικό κάθε κτηρίου μπορεί να έχει πρόσβαση στο DATABASESERVER(ΟΠΣ ΤΟΥ ΔΗΜΟΥ ΤΗΣ ΕΤΑΙΡΙΑΣ ΟΤS) που βρίσκεται στο κεντρικό Δημαρχείο και να ενημερώνει τα αρχεία της βάσης δεδομένων ως ένα υπηρεσιακό δίκτυο WAN μέσω Σύζευξης

Υλικό – Λογισμικό Συστήματος:

Με απόφαση δημάρχου σε φύλλο excel καταγράφεται ο εξοπλισμός πληροφορικής που περιλαμβάνει το όνομα χρήστη, τα τεχνικά χαρακτηριστικά του Η/Υ (cpu, ram, Όνομα, IP, MAC Address κλπ), αλλά και των εκτυπωτών, του λειτουργικού συστήματος και των εφαρμογών γραφείου που είναι εγκατεστημένα στον κάθε υπολογιστή κάθε κτηρίου από τα παραπάνω.

Το Γραφείο ΤΠΕ, συνεργάζεται με το τεχνικό προσωπικό του Σύζευξης για την επίλυση προβλημάτων στο ίντερνετ-τηλεφωνία-ταχύτητες διασύνδεσης και αναλαμβάνει (χωρίς συμβάσεις υποστήριξης από εξωτερικούς οικονομικούς φορείς) τη συντήρηση του εξοπλισμού των υπολογιστών, την αναβάθμιση, την εγκατάσταση των εφαρμογών και επιλύει προβλήματα εσωτερικής δικτύωσης του κάθε κτηρίου. Υπάρχει σύμβαση υποστήριξης για τη συντήρηση των εκτυπωτών – φωτοτυπικών και μία πρόβλεψη για σύμβαση για την υποστήριξη επιδιόρθωσης των οθονών και των UPS.

Υπάρχουν οι παρακάτω διακομιστές δικτύου στο Κεντρικό Κτήριο του Δήμου

1. Domain Controller 1
2. Domain Controller 2
3. File Server (NAS)
4. Database Server Εφαρμογών της Oracletης εταιρίας OTS
5. Παλαιός Server Εφαρμογών του Δήμου Αριδαίας πριν την συνένωση του Καλλικράτη στους Δήμους
6. Παλαιός Εικονικός Servertου Δήμου Εξαπλατάνου πριν την συνένωση του Καλλικράτη στους Δήμους

Έχει προβλεφθεί για το επόμενο έτος η μετάπτωση των server 4,5,6 σε ένα Server εφαρμογών, σύγχρονο που έχει ήδη αγορασθεί.

Ο ρόλος των Domain Controller 1 και 2 είναι να επιτυγχάνεται αφενός η ταυτοποίηση των χρηστών με κωδικό πρόσβασης και αφετέρου η εξουσιοδοτημένη πρόσβαση στο File Server (NAS) σε κοινόχρηστους φακέλους με πρόσβαση (εγγραφής, ανάγνωσης) σύμφωνα τη δομή του οργανογράμματος του Δήμου.

Ο κωδικός πρόσβασης των χρηστών έχει υποχρεωτικά μήκος τουλάχιστον 6 χαρακτήρων και δεν ακολουθεί άλλες πολιτικές πολυπλοκότητας είτε υποχρεώσεις αλλαγών σε τακτά χρονικά διαστήματα.

Οι υπολογιστές διαθέτουν όλοι λειτουργικό σύστημα Windows 10 ή 11 και οι ελάχιστοι που διαθέτουν Windows 7 έχουν αγορασθεί τερματικά με Windows 11 τα οποία και θα τους αντικαταστήσουν. Στους υπολογιστές υπάρχουν άδειες προεγκατεστημένες των Windows, είναι πλήρως ενημερωμένοι και διαθέτουν αντιικό πρόγραμμα και τείχος προστασίας.

Ο Δήμος έχει αγοράσει, αρκετές και συνεχώς σε ετήσια βάση επιπλέον άδειες για τη σουίτα εφαρμογών του Office, ενώ πρόσφατα ανανέωσε για δεύτερη συνεχόμενη τριετία το λογισμικό Autocad Light 2023 για το Τμήμα Τεχνικών Υπηρεσιών.

Υπάρχουν αρχεία καταγραφής (logfiles) σε όλους τους Serverκαι μπορούν να αναζητηθούν στοιχεία σφαλμάτων αν χρειαστεί.

Λογισμικό εφαρμογών (προγράμματα)

Στο Δήμο Αλμωπίας έχουν αποδοθεί 40 συνολικά άυλες – απομακρυσμένες ψηφιακές υπογραφές και έχουν ενεργοποιηθεί οι περισσότερες μέσω OTP στο κινητό των δικαιούχων

Ακολουθεί λίστα με το λογισμικό εφαρμογών που χρησιμοποιείται από τις Υπηρεσίες του Δήμου Αλμωπίας.

1. Διαχείρισης Οικονομικού
2. Οικονομική Διαχείριση - Υποσύστημα Δημοσίευσης στη Διαύγεια
3. Οικονομική Διαχείριση - Υποσύστημα Διαχείρισης Συμβάσεων
4. Μισθοδοσία
5. Διαχείριση Προσωπικού
6. Ενιαία Αρχή Πληρωμών
7. Ηλεκτρονικό Πρωτοκόλλου WEB
8. Open1 –Property για την διαχείριση του ΤΑΠ
9. Διαχείρισης Δημοτικού Φόρου
10. Διαχείρισης Στόλου Οχημάτων Desktop
11. Διαχείριση Έργων
12. ΣΗΔΕ – Tukanga και διασύνδεση με ΚΣΗΔΕ του Υπ. Ψηφιακής Διακυβέρνησης

Στο Δήμο υπάρχει ιστοσελίδα που λειτουργεί ως ηλεκτρονική εφημερίδα ανακοινώσεων. Η μόνη δυνατότητα διαδραστικής επικοινωνίας με τους πολίτες είναι η αποστολή μηνύματος από την καρτέλα Επικοινωνία στο κεντρικό email της Υπηρεσίας

Στο Δήμο έχουν ανατεθεί κωδικοί χρήσης για το πρόγραμμα ΗΡΙΔΑ του ΥΠΕΣ για την επικοινωνία με το Υπουργείο, την Αποκεντρωμένη Διοίκηση και τους άλλους Δήμους της χώρας.

Στο Δήμο έχουν ανατεθεί κωδικοί χρήσης για όλες τις διαθέσιμες εφαρμογές του GOVHUB της ΚΕΔΕ όπως αναφέρονται παρακάτω, για την άμεση ενημέρωση των υπηρεσιών:

1. ΒΕΒΑΙΩΣΕΙΣ ΜΟΝΙΜΟΥ ΚΑΤΟΙΚΙΑΣ
2. ΠΕΛΟΠΑΣ
3. ΔΙΟΡΘΩΣΕΙΣ ΤΕΤΡΑΓΩΝΙΚΩΝ ΜΕΤΡΩΝ
4. ΦΟΡΟΛΟΓΙΚΗ ΕΝΗΜΕΡΟΤΗΤΑ
5. ΠΟΙΝΙΚΟ ΜΗΤΡΩΟ
6. ΚΑΤΟΧΟΙ ΟΧΗΜΑΤΩΝ
7. ΑΚΙΝΗΤΗ ΠΕΡΙΟΥΣΙΑ Ε9
8. ΜΗΤΡΩΟ ΦΥΣΙΚΩΝ ΠΡΟΣΩΠΩΝ
9. ΑΠΑΛΛΑΓΗ ΤΕΛΟΥΣ ΚΟΙΝΟΧΡΗΣΤΩΝ ΧΩΡΩΝ
10. ΑΚΑΘΑΡΙΣΤΑ ΕΣΟΔΑ ΓΙΑ ΠΑΡΕΠΙΔΗΜΟΥΝΤΕΣ

Στο Δήμο έχουν ανατεθεί Κωδικοί Δημόσιας Διοίκησης για την εξυπηρέτηση απομακρυσμένων ηλεκτρονικών αιτήσεων πολιτών μέσω του gov.gr στο ΚΕΠ, στο Δημοτολόγιο, στο Ληξιαρχείο και στο Πρωτόκολλο του Δήμου και μπορούν να εξυπηρετούν ότι άλλο προστεθεί στην πλατφόρμα του gov.gr για την εξυπηρέτηση των πολιτών.

Αντίγραφα ασφαλείας

Αντίγραφα τηρούνται καθημερινά τόσο στο Server των εφαρμογών της εταιρίας OTS όσο και στο FileServer με την τεχνική του mirroring σε εξωτερικό δίσκο.

Φυσική ασφάλεια χώρου:

Υπάρχει σύμβαση για την αγορά πόρτας για να κλειδωθεί ο χώρος του Server Room στον οποίο η υπάρχουσα πόρτα έχει φθαρεί από πλημμύρα που υπέστη ο χώρος του server. Δεν υπάρχει Μονάδα Η/Ζ παρά μόνο UPS

σε κάθε υπολογιστή, δεν υπάρχει σύστημα πυρανίχνευσης, αισθητήρες καπνού ή φωτιάς, παρά μόνο πυροσβεστήρες κατανεμημένοι σε διάφορους χώρους.

2. Μεθοδολογία

Περιγραφή

Σύμφωνα με την σειρά διεθνών προτύπων ασφάλειας ISO27000, η ασφάλεια πληροφοριακών συστημάτων, ορίζεται από τις παρακάτω συνιστώσες:

- Εμπιστευτικότητα (Confidentiality): η πληροφορία παραμένει μυστική, διαθέσιμη μόνο σε εξουσιοδοτημένες οντότητες.
- Ακεραιότητα(Integrity):Η πληροφορία παραμένει αναλλοίωτη, για παράδειγμα δεν μεταβάλλεται από μη εξουσιοδοτημένες οντότητες.
- Διαθεσιμότητα(Availability):η πληροφορία και οι υπηρεσίες που παρέχει το σύστημα βρίσκεται στην διάθεση των χρηστών του πληροφοριακού συστήματος όταν εκείνοι την χρειάζονται.

Για την ανάλυση επικινδυνότητας κατά την διαδικασία ανάπτυξης και χρήσης ενός πληροφοριακού συστήματος:

1. Ορίζουμε τις απειλές.
2. Ορίζουμε επίπεδα/ κατηγορίες κρισιμότητας.
3. Διεξάγουμε Ανάλυση Επίδρασης Απειλών, ώστε να κατανοήσουμε το αντίκτυπο από την πραγματοποίηση ενός περιστατικού ασφάλειας ανά πληροφορία και με τελικό στόχο την κατηγοριοποίηση των υποσυστημάτων σε επίπεδα κρισιμότητας.
4. Διεξάγουμε ανάλυση επικινδυνότητας εντοπίζοντας αδυναμίες ασφάλειας. Μελετώνται επίσης οι προδιαγραφές ασφάλειας που συστήνουν τα διεθνή πρότυπα ώστε να εξασφαλίσουμε ότι όλες οι κατηγορίες αδυναμιών καλύπτονται.
5. Για την επίτευξη του τελικού στόχου (ανάδειξη πολιτικής και μέτρων ασφάλειας) η ανάλυση επικινδυνότητας συνδυάζει τα αποτελέσματα της ανάλυσης επίδρασης με τις αδυναμίες (οι οποίες με τη σειρά τους επηρεάζουν την πιθανότητα πραγματοποίησης περιστατικού ασφάλειας) ώστε να εξάγει το επίπεδο κινδύνου. Υπολογίζουμε το επίπεδο κινδύνου ανά υποσύστημα σύμφωνα με την παρακάτω εξίσωση:

Κίνδυνος = Επίπεδο Κρισιμότητας (αξία) x Πιθανότητα λόγω

3. Ορισμός απειλών

Γενικές Απειλές

Οι απειλές κατηγοριοποιούνται σε τρεις βασικές κατηγορίες, αντίστοιχες των θεμελιωδών αρχών ασφάλειας των πληροφοριακών συστημάτων, οι οποίες παρουσιάζονται στον παρακάτω πίνακα. Η περιγραφή κάθε απειλής είναι ενδεικτική.

Αρ.	Απειλή	Σύντομη περιγραφή των ενδεχομένων συνεπειών
A1	Παραβίαση εμπιστευτικότητας πληροφορίας	Πιθανές συνέπειες αφορούν σε δυσφήμηση, νομικές κυρώσεις και οικονομικές κυρώσεις, από τη μη τήρηση συμβάσεων εμπιστευτικότητας με τρίτους ή απαιτήσεων του νομικού πλαισίου (για παράδειγμα προσωπικά δεδομένα).
A2	Απώλεια ακεραιότητας πληροφορίας	Η αλλοίωση εγγραφών ή δεδομένων μπορεί να φέρει σημαντικό αρνητικό αντίκτυπο, συμπεριλαμβανομένης της δυσφήμησης του Δήμου Αλμωπίας και πιθανώς νομικές και οικονομικές κυρώσεις (αν για παράδειγμα αποτελέσει μέσο απάτης).
A3	Απώλεια διαθεσιμότητας πληροφορίας	Πιθανές συνέπειες από απώλεια διαθεσιμότητας σχετίζονται με τις υποχρεώσεις του Δήμου Αλμωπίας για την διεξαγωγή των σχετικών διεργασιών που υποστηρίζει το πληροφοριακό σύστημα. Ποικίλουν από δυσφήμηση, μέχρι πιθανές νομικές ή συμβατικές κυρώσεις.

Ειδικές απειλές

Σενάρια φυσικών καταστροφών

Καταστροφή	Σύντομη περιγραφή των ενδεχομένων συνεπειών
Σεισμός	Ισχυροί σεισμοί μπορούν να καταστρέψουν την ηλεκτρική ισχύ και τις γραμμές επικοινωνίας και να διακόψουν την παροχή νερού και του αποχετευτικού συστήματος. Μπορεί να προκληθεί σημαντική καταστροφή στις εγκαταστάσεις του Δήμου Αλμωπίας, συμπεριλαμβανομένης και της ολικής κατάρρευσης κτιρίων. Οι σεισμοί μπορούν επίσης να προκαλέσουν εδαφικές καθιζήσεις.

Πυρκαγιά	Οι πυρκαγιές είναι επίσης καταστροφικές και μπορεί να ξεκινήσουν από ένα μεγάλο αριθμό περιστατικών τα οποία ίσως να είναι συμπτωματικά. Την δριμύτητα της φωτιάς και την ταχύτητα εξάπλωσής της. Η πυρκαγιά μπορεί να προκαλέσει ανθρώπινο τραυματισμό ή θάνατο και καταστροφή σε αρχεία και εξοπλισμό, καθώς και στην δομή των κτιριακών εγκαταστάσεων.
Πλημμύρα	Πλημμύρες προέρχονται από θύελλες, καταιγίδες, ή βαριά και εκτεταμένη βροχόπτωση που είναι η αιτία να πλημμυρίζουν οι γύρω περιοχές. Οι πλημμύρες μπορούν να επιδράσουν σοβαρά στα κτίρια και τον εξοπλισμό προκαλώντας ανεπάρκεια στην ηλεκτρική ισχύ και απώλεια των κτιριακών υπηρεσιών.
Κεραυνοί	Το αντίκτυπο των κεραυνών μπορεί να είναι σημαντικό. Μπορεί να προκαλέσει διακοπή ρεύματος, να καταστρέψει τον ηλεκτρικό εξοπλισμό και τα υπολογιστικά συστήματα. Η οικοδομική καταστροφή είναι επίσης πιθανή, λόγω της πτώσης δέντρων και άλλων αντικειμένων.

Σενάρια οργανωμένης ή εσκεμμένης επίθεσης

Καταστροφή	**Σύντομη περιγραφή των ενδεχομένων συνεπειών**
Τρομοκρατική ενέργεια-τοποθέτηση εκρηκτικού μηχανισμού	Οι τρομοκρατικές ενέργειες περιλαμβάνουν εκρήξεις, απειλές με βόμβες, ομήρους, δολιοφθορά, και οργανωμένη βία. Είτε αυτό ετοιμάζεται από αναγνωρισμένο τρομοκράτη, οργανισμό, ή ομάδα διαμαρτυρίας, η επιρροή στο Δήμο Αλμωπίας είναι η ίδια.
Ενέργεια δολιοφθοράς	Μία ενέργεια δολιοφθοράς είναι η εσκεμμένη διακοπή των δραστηριοτήτων του Δήμου Αλμωπίας. Η εργασία θα επηρεαστεί σημαντικά και άμεσα από επιτυχημένες απόπειρες για σαμποτάζ. Αυτό μπορεί να επηρεάσει τις φυσιολογικές λειτουργίες και να οδηγήσει στην αποσταθεροποίηση του εργατικού δυναμικού.
Κλοπή/βανδαλισμός	Η κλοπή ποικίλει από την κλοπή αγαθών ή εξοπλισμού μέχρι και κλοπή άλλων αντικειμένων αξίας(συμπεριλαμβανομένης της πληροφορίας).
Εμπρησμός	Ο εμπρησμός είναι η εσκεμμένη απόπειρα πυρκαγιάς με σκοπό την καταστροφή των κτιριακών εγκαταστάσεων, του εξοπλισμού και των περιεχομένων του Δήμου Αλμωπίας Κάτι τέτοιο μπορεί να προκαλέσει τόσο απώλεια των κτιριακών εγκαταστάσεων όσο και των αγαθών και γενικά και άλλων περιουσιακών στοιχείων του Δήμου Αλμωπίας.

Απεργίες/Καταλήψεις	Αυτό το είδος ενέργειας επηρεάζει τη λειτουργία του συστήματος καθώς το προσωπικό δεν είναι σε θέση να υποστηρίξει τα πληροφοριακά συστήματα του Δήμου Αλμωπίας για την κανονική τους λειτουργία.

Σενάρια απώλειας πόρων και υπηρεσιών

Καταστροφή	**Σύντομη περιγραφή των ενδεχομένων συνεπειών**
Απώλεια ηλεκτρικής ισχύος	Όλα τα πληροφοριακά συστήματα εξαρτώνται από την ηλεκτρική ισχύ προκειμένου να συνεχίσουν τις φυσιολογικές τους λειτουργίες. Χωρίς ηλεκτρική ισχύ οι υπολογιστές, τα φώτα, τα τηλέφωνα και άλλα μέσα επικοινωνίας δεν θα λειτουργούν με αντίκτυπο στην ομαλή διεξαγωγή των εργασιών.
Έλλειψη πετρελαίου	Για τις περισσότερες χώρες στον κόσμο, μία πετρελαϊκή έλλειψη/κρίση μπορεί να εμφανισθεί ανά πάσα στιγμή. Κάτι τέτοιο έχει σημαντικό αντίκτυπο στην διεξαγωγή των εργασιών επηρεάζοντας άμεσα τα μεταφορικά μέσα και τις φυσιολογικές λειτουργίες των μηχανών που κινούνται/λειτουργούν με βενζίνη ή πετρέλαιο (πχ ένα ηλεκτροπαραγωγό ζεύγος).
Κατάρρευση Τηλεπικοινωνιακών υπηρεσιών	Μία διακοπή στις τηλεπικοινωνιακές υπηρεσίες μπορεί να επηρεάσει τη φυσιολογική λειτουργία του Δήμου Αλμωπίας, πολλές από τις υπηρεσίες οι οποίες βασίζονται σε τηλεπικοινωνιακά δίκτυα.

Σενάρια βλάβης εξοπλισμού ή συστήματος

Καταστροφή	**Σύντομη περιγραφή των ενδεχομένων συνεπειών**
Εσωτερική απώλεια ενέργειας	Μια εσωτερική απώλεια ενέργειας είναι μια διακοπή στις διαδικασίες των υπηρεσιών παροχής ηλεκτρικής ενέργειας, που προκαλείται από βλάβη εσωτερικού εξοπλισμού ή καλωδίωσης. Αυτό το είδος βλάβης θα πρέπει να επισκευάζεται από εξειδικευμένο ηλεκτρολόγο και οι καθυστερήσεις αναπόφευκτα θα έχουν επίπτωση στη λειτουργία του Δήμου Αλμωπίας Όπου έχουν συμβεί ιδιαίτερα σημαντικές βλάβες, όπως ζημιές σε κεντρικά καλώδια, οι επισκευές θα μπορούσαν να διαρκέσουν αρκετό χρόνο και μπορεί να έχουν σοβαρό αντίκτυπο στη λειτουργία του οργανισμού.
Βλάβη στο σύστημα	Μια βλάβη του συστήματος κλιματισμού θα μπορούσε να έχει σοβαρές επιπτώσεις όπου η μονάδα κλιματισμού προστατεύει ιδιαίτερα ευαίσθητο εξοπλισμό, (πχ κέντρα δεδομένων) και η αύξηση της θερμοκρασίας θα μπορούσε να προκαλέσει βλάβη στον εξοπλισμό. Μπορεί επίσης να επηρεάσει το εργατικό δυναμικό καθώς οι συνθήκες στο κτίριο μπορεί να γίνουν

	εξαιρετικά ανυπόφορες από μια σημαντική άνοδο της θερμοκρασίας και το προσωπικό να επηρεαστεί αρνητικά.

Σενάρια συμβάντων πληροφοριακής ασφάλειας

Καταστροφή	**Σύντομη περιγραφή των ενδεχομένων συνεπειών**
Αποκάλυψη Ευαίσθητης πληροφορίας	Αποτελεί ένα σοβαρό συμβάν ασφάλειας, το οποίο μπορεί να προκαλέσει σοβαρές νομικές κυρώσεις, καθώς τα πληροφοριακά συστήματα του Δήμου Αλμωπίας ενδεχομένως να περιλαμβάνουν και ευαίσθητα προσωπικά δεδομένα πολιτών.
Απώλεια εγγράφων ή δεδομένων	Η απώλεια εγγραφών ή δεδομένων μπορεί να προκαλέσει ιδιαίτερη παρακώλυση όπου οι ανεπαρκείς διαδικασίες τήρησης αντιγράφων ασφαλείας και ανάκτησης δεδομένων έχουν ως αποτέλεσμα την επανεισαγωγή και την επανεπεξεργασία των εγγραφών. Αυτή είναι φυσιολογικά μια αργή και ιδιαίτερα εντατική διαδικασία.
Βλάβη πληροφοριακών συστημάτων	Λαμβάνοντας υπόψη την εξάρτηση από τα πληροφοριακά συστήματα του Δήμου Αλμωπίας, της συντριπτικής πλειοψηφίας των λειτουργιών, μια βλάβη σε ένα από αυτά, μπορεί να είναι ιδιαίτερα καταστροφική. Τα είδη των απειλών των υπολογιστικών συστημάτων είναι πολλά και ποικίλα, και συμπεριλαμβάνουν, βλάβη σε υπολογιστικό υλικό, ζημιά σε καλώδια, διαρροές νερού και φωτιές, βλάβες των συστημάτων κλιματισμού, βλάβες του δικτύου, βλάβες των συστημάτων εφαρμογών, βλάβες τηλεπικοινωνιακού εξοπλισμού, κτλ.

Ορισμός κατηγοριών κρισιμότητας

Στη παράγραφο αυτή ορίζουμε τις κατηγορίες κρισιμότητας, βάσει των οποίων θα ταξινομηθούν τα αγαθά των πληροφοριακών συστημάτων. Η κρισιμότητα, εξαρτάται από την έκταση της ανάγκης υποστήριξης των θεμελιωδών υπηρεσιών ασφάλειας: **διαθεσιμότητα, εμπιστευτικότητα και ακεραιότητα**, άρα και από την ανάγκη για προστασία από την πραγματοποίηση των αντίστοιχων απειλών, οι οποίες θα έχουν συγκεκριμένες επιπτώσεις.

Κατηγορία	Περιγραφή
Υψηλό	Η διατήρηση της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας του συστήματος/λειτουργίας **είναι ύψιστης σημασίας**.
Μέσο	Η διατήρηση της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας του συστήματος/λειτουργίας **είναι σημαντική**.
Χαμηλό	Η διατήρηση της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας του συστήματος/λειτουργίας **είναι μειωμένης σημασίας**.

Υπολογισμός Κινδύνου

Ο παρακάτω πίνακας παρουσιάζει την υλοποίηση της εξίσωσης υπολογισμού τελικού επιπέδου κινδύνου.

		Επίπεδο Επικινδυνότητας(πιθανότητα λόγω αδυναμιών)		
		Υψηλό	**Μέσο**	**Χαμηλό**
Κρισιμότητα Υποσυστήματος	**Υψηλό**	*Υψηλό*	*Υψηλό*	*Μέσο*
	Μέσο	*Υψηλό*	*Μέσο*	*Χαμηλό*
	Χαμηλό	**Μέσο**	*Χαμηλό*	*Χαμηλό*

4. Ανάλυση Επίδρασης και Κατηγοριοποίηση Υποσυστημάτων και Πληροφορίας

Λαμβάνοντας υπόψη τις απειλές, αλλά και τις συνέπειες που θα προκαλέσει η πιθανή πραγματοποίηση κάθε απειλής, μπορούμε να ορίσουμε το επίπεδο κρισιμότητας των πληροφοριακών συστημάτων. Η διαβάθμιση έχει ως στόχο τον ορισμό προτεραιοτήτων ασφάλειας ανάμεσα στα συστατικά των πληροφοριακών συστημάτων του Δήμου Αλμωπίας, λαμβάνοντας υπόψη ότι τα πληροφοριακά συστήματα του Δήμου Αλμωπίας αποτελούν κρίσιμο στοιχείο της υποδομής της και η αποτελεσματική λειτουργία τους συνδέεται άρρηκτα με την αποτελεσματική λειτουργία του Δήμου Αλμωπίας.

Αποτίμηση κινδύνων Υποθέσεις και μέτρα ασφαλείας

Δήμος Αλμωπίας Αποτίμηση κινδύνων

Πλήρη διαχωρισμό των επιπέδων των πληροφοριακών συστημάτων (επίπεδο εφαρμογών, επίπεδο βάσης δεδομένων, επίπεδο παγκόσμιου ιστού) σε διαφορετικούς εξυπηρετητές ώστε ζώνες διαφορετικής κρισιμότητας να προστατεύονται ανάλογα, μειώνοντας την «επιφάνεια» και συνεπώς τον αντίκτυπο, πιθανών

επιθέσεων. Ο κίνδυνος μη διαθεσιμότητας υφίσταται στο ότι ο πλήρης διαχωρισμός των επιπέδων πληροφοριακών συστημάτων σε διαφορετικούς εξυπηρετητές προσφέρει ουσιαστικά πλεονεκτήματα σε όρους ασφάλειας, απόδοσης και διαχείρισης. Με τη μείωση της επιφάνειας επίθεσης και τον περιορισμό του αντίκτυπου πιθανών επιθέσεων, ενισχύεται η συνολική ανθεκτικότητα και ασφάλεια του συστήματος. Επίπεδο επικινδυνότητας: ΧΑΜΗΛΟ

Χρήση τεχνικών υψηλής διαθεσιμότητας (highavailability). Ο κίνδυνος μη διαθεσιμότητας λόγω τεχνικής βλάβης μπορεί να προκαλέσει διακοπές στις υπηρεσιακές διαδικασίες, απώλεια δεδομένων, μείωση της αξιοπιστίας και της εμπιστοσύνης των πολιτών, καθώς και οικονομικές απώλειες. Επίπεδο επικινδυνότητας: ΜΕΣΟ

Ισχυρός μηχανισμός διαχείρισης πρόσβασης χρηστών βάσει ρόλων υποστηριζόμενος από ασφαλείς μεθόδους χρήσης συνθηματικών, ψηφιακά πιστοποιητικά/τεκμήρια πιστοποίησης ταυτότητας (2-factor authentication). Ο κίνδυνος μη διαθεσιμότητας μπορεί να προκαλέσει απώλεια ευαίσθητων αρχείων και δεδομένων ή πρόσβαση σε ευαίσθητα αρχεία και δεδομένα από μη εξουσιοδοτημένους χρήστες με κακόβουλες προθέσεις. Επίπεδο επικινδυνότητας: ΧΑΜΗΛΟ.

Υποδομή φυσικής προστασίας πληροφοριακών συστημάτων, σύστημα αδιάλειπτης παροχής ηλεκτρικής ενέργειας(UPS). Ο κίνδυνος μη διαθεσιμότητας μπορεί να προκαλέσει απώλεια δεδομένων, διακοπή υπηρεσιών, υποβάθμιση επίδοσης και ζημίες στον εξοπλισμό. Επίπεδο επικινδυνότητας: ΧΑΜΗΛΟ.

Υποδομή τήρησης αντιγράφων ασφαλείας (backup). Ο κίνδυνος μη διαθεσιμότητας μπορεί να προκαλέσει δυσλειτουργία συστημάτων, απώλεια δεδομένων και οικονομικές απώλειες σε περίπτωση καταστροφής φυσικής και μη. Επίπεδο επικινδυνότητας: ΧΑΜΗΛΟ.

Υποδομή δευτερεύοντος συστήματος για αντιμετώπιση καταστροφών. Η μη διαθεσιμότητα της δευτερεύουσας υποδομής μπορεί να οδηγήσει σε απώλεια λειτουργικότητας και σε σοβαρές συνέπειες για τον οργανισμό, όπως αδυναμία παροχής υπηρεσιών προς τους πολίτες, οικονομικές απώλειες ή ακόμη και κίνδυνο για την ανθρώπινη ασφάλεια. Επίπεδο επικινδυνότητας: ΜΕΣΟ.

Υποδομή δικτυακής ασφάλειας (firewall). Ο κίνδυνος μη διαθεσιμότητας μπορεί να οδηγήσει σε επιθέσεις από το διαδίκτυο, διαρροές δεδομένων, μειωμένη προστασία από εσωτερικές απειλές και απώλεια σημαντικών ρυθμίσεων ασφαλείας. Επίπεδο επικινδυνότητας: ΧΑΜΗΛΟ.

Μηχανισμοί επαναφοράς σε προηγούμενη κατάσταση των δεδομένων (rollback). Ο κίνδυνος μη διαθεσιμότητας εκθέτει τον οργανισμό σε σοβαρούς κινδύνους, συμπεριλαμβανομένης της δυσκολίας αντιμετώπισης σφαλμάτων, της απώλειας συνέπειας στο σύστημα και της απειλής για την ασφάλεια των δεδομένων. Επίπεδο επικινδυνότητας: ΜΕΣΟ

Φυσική ασφάλεια. Η ηλεκτρική ισχύ είναι πολύ χαμηλή και ασταθής στο Δήμο Αλμωπίας και δε μπορεί να εξυπηρετήσει τις υπάρχουσες ανάγκες. Οι υπολογιστές, τα συστήματα ψύξης, τα φώτα, τα τηλέφωνα και άλλα μέσα δεν λειτουργούν ικανοποιητικά και αυτό έχει αντίκτυπο στην ομαλή διεξαγωγή των εργασιών και την φυσική προστασία των servers.
Μια βαριά και εκτεταμένη βροχόπτωση μπορεί να αποτελέσει αιτία να πλημμυρίζουν οι χώροι των servers στο Δημαρχείο. Οι πλημμύρες μπορούν να επιδράσουν σοβαρά στα κτίρια και τον εξοπλισμό προκαλώντας ανεπάρκεια στην ηλεκτρική ισχύ και απώλεια των κτιριακών υπηρεσιών. Μια εσωτερική απώλεια ενέργειας είναι μια διακοπή στις διαδικασίες των υπηρεσιών παροχής ηλεκτρικής ενέργειας, που προκαλείται από βλάβη εσωτερικού εξοπλισμού ή καλωδίωσης. Η πυρασφάλεια, η προστασία από πλημμύρα, ο κλιματισμός, ο εξαερισμός, ο φυσικός έλεγχος φυσικής πρόσβασης με κάρτες, η παρακολούθηση περιβάλλοντος, ο συναγερμός είναι θέματα που πρέπει να επιλυθούν διότι αποτελούν παράγοντες σημαντικής επικινδυνότητας.
Επίπεδο επικινδυνότητας: ΥΨΗΛΟ

Τα ακόλουθα προτεινόμενα μέτρα ασφάλειας θα πρέπει να λαμβάνονται υπόψη σε κάθε ανάλυση επικινδυνότητας, η οποία θα πρέπει να επαναλαμβάνεται σε τακτά χρονικά διαστήματα:

- Πλήρης διαχωρισμός των επιπέδων των πληροφοριακών συστημάτων (επίπεδο εφαρμογών, επίπεδο βάσης δεδομένων, επίπεδο παγκόσμιου ιστού) σε διαφορετικούς εξυπηρετητές ώστε ζώνες διαφορετικής κρισιμότητας να προστατεύονται ανάλογα, μειώνοντας την «επιφάνεια» και συνεπώς τον αντίκτυπο, πιθανών επιθέσεων (Έντυπο 2:Πολιτική ασφαλείας διακομιστών (servers)).

- Χρήση τεχνικών υψηλής διαθεσιμότητας (highavailability) (Έντυπο 2:Πολιτική ασφαλείας διακομιστών (servers)).

- Ισχυρός μηχανισμός διαχείρισης πρόσβασης χρηστών βάσει ρόλων υποστηριζόμενος από ασφαλείς μεθόδους χρήσης συνθηματικών, ψηφιακά πιστοποιητικά/τεκμήρια πιστοποίησης ταυτότητας(2-factor authentication)(Έντυπο 2:Πολιτική ασφαλείας σταθμών εργασίας με ευαίσθητα δεδομένα).

- Υποδομή φυσικής προστασίας πληροφοριακών συστημάτων, σύστημα αδιάλειπτης παροχής ηλεκτρικής ενέργειας (UPS), πυρασφάλεια, προστασία από πλημμύρα, κλιματισμός, εξαερισμός, έλεγχος φυσικής πρόσβασης με κάρτες, παρακολούθηση περιβάλλοντος, συναγερμός.(Έντυπο 2:Πολιτική ασφαλείας διακομιστών (servers)).

- Υποδομή τήρησης αντιγράφων ασφαλείας (backup)(Έντυπο 2:Πολιτική ασφαλείας διακομιστών (servers)).

- Υποδομή δευτερεύοντος συστήματος για αντιμετώπιση καταστροφών (Έντυπο 2:Πολιτική ασφαλείας διακομιστών (servers)).

- Υποδομή δικτυακής ασφάλειας(firewall)(Έντυπο 2:Πολιτική χρήσης-φιλτραρίσματος διαδικτύου).

- Μηχανισμοί καταγραφής αλλαγών και τήρησης ιστορικών αρχείων(audit/logfiles)(Έντυπο 2:Πολιτική ασφαλείας διακομιστών (servers)).

- Μηχανισμοί επαναφοράς σε προηγούμενη κατάσταση των δεδομένων (rollback) (Έντυπο 2:Πολιτική ασφαλείας διακομιστών (servers)).

- Χρήση ασφαλών πρωτοκόλλων επικοινωνίας υποστηριζόμενων από κρυπτογραφία (TLS/SSL,HTTPS)(Έντυπο 2:Πολιτική χρήσης-φιλτραρίσματος διαδικτύου).

Λειτουργική συνέχεια του Εντύπου 1 με το Έντυπο 2.

Οι πολιτικές Ασφάλειας Υπολογιστών και Δικτύων Υπηρεσιών του Δήμου Αλμωπίας σε ξεχωριστό έντυπο στο Έντυπο 2 περιορίζονται σε κινδύνους και θέματα που σχετίζονται κυρίως με τα πληροφοριακά συστήματα του Δήμου Αλμωπίας. Σκοπός η αποφυγή κοινών σημείων με άλλα σχετικά έγγραφα που περιγράφουν ισχύοντες κανονισμούς του Δήμου Αλμωπίας, ενώ σε άλλα λειτουργεί συμπληρωματικά με αρμοδιότητες και συστήματα που εμπίπτουν στις αρμοδιότητες άλλων Τμημάτων του Δήμου Αλμωπίας όπως:

1. Τμήμα Διοικητικών Υπηρεσιών (Τεχνικός Ασφαλείας).

2. Τμήμα Τεχνικών Υπηρεσιών (Ηλεκτρολογική Εγκατάσταση, Πυρασφάλεια, πυρκαγιά, πλημμύρες κλπ).

3. Τμήμα Περιβάλλοντος, Πολιτική Προστασία (Πυρασφάλεια, πυρκαγιά, πλημμύρες κλπ).

Στα ανωτέρω συστήματα δεν παρεμβαίνει η πρόταση του παρόντος Κανονισμού.

ΔΗΜΟΣ ΑΛΜΩΠΙΑΣ

ΤΜΗΜΑ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥΟΡΓΑΝΩΣΗΣ & ΠΛΗΡΟΦΟΡΙΚΗΣ ΔΗΜΟΥ ΑΛΜΩΠΙΑΣ
ΓΡΑΦΕΙΟ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΕΠΙΚΟΙΝΩΝΙΩΝ

ΚΑΝΟΝΙΣΜΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΔΗΜΟΥ ΑΛΜΩΠΙΑΣ

ΕΝΤΥΠΟ 2

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ & ΔΙΚΤΥΩΝ

ΥΠΗΡΕΣΙΩΝ ΔΗΜΟΥ ΑΛΜΩΠΙΑΣ

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ & ΔΙΚΤΥΩΝ ΥΠΗΡΕΣΙΩΝ ΔΗΜΟΥ ΑΛΜΩΠΙΑΣ

Περιεχόμενα 1

Πολιτική χρήσης-φιλτραρίσματος διαδικτύου

Πολιτική:

- Η αρχική πρόσβαση στο διαδίκτυο θα χορηγείται μέσω της αίτησης στον υπεύθυνο ασφαλείας.
- Οι χρήστες θα ενημερώνονται για τη σωστή και αποτελεσματική χρήση του διαδικτύου.
- Οι χρήστες θα έχουν πρόσβαση στο διαδίκτυο χρησιμοποιώντας μόνο εγκεκριμένη υποδομή των πληροφοριακών συστημάτων του Δήμου Αλμωπίας.
- Ο Δήμος Αλμωπίας δεν φέρει καμία ευθύνη για τις απόψεις που εκφράζουν οι χρήστες στο διαδίκτυο.
- Οι χρήστες θα ενημερώνονται ώστε να μη κατεβάζουν ή μεταδίδουν υλικό που είναι προσβλητικό- παράνομο.
- Οι εσωτερικές IP διευθύνσεις που χρησιμοποιούνται στο πληροφοριακό σύστημα θα πρέπει να είναι εμπιστευτικές.
- Όλα τα ύποπτα αρχεία επισυναπτόμενα ηλεκτρονικού ταχυδρομείου που κατεβάζουν οι χρήστες από το διαδίκτυο θα περνάνε από αυστηρό έλεγχο πριν χρησιμοποιηθούν.
- Οι χρήστες θα ενημερώνουν τον υπεύθυνο ασφάλειας για οποιοδήποτε περιστατικό εισβολής.
- Τείχος προστασίας (Firewall)
- Πρωτόκολλα επικοινωνίας (TLS/SSL,HTTPS)

Συμμόρφωση Πολιτικής:

- Η λειτουργία και η χρήση των πληροφοριακών συστημάτων του Δήμου Αλμωπίας υπόκειται σε κανονισμούς, νόμους και αρχές που αφορούν σε θέματα ασφάλειας, που πρέπει να τηρούνται.
- Όλο το προσωπικό των χρηστών των πληροφοριακών συστημάτων του Δήμου Αλμωπίας, καθώς και όλοι οι εμπλεκόμενοι με το σύστημα φορείς οφείλουν να συμμορφώνονται με την πολιτική ασφάλειας των πληροφοριακών συστημάτων.
- Η πολιτική ασφάλειας των πληροφοριακών συστημάτων του Δήμου Αλμωπίας πρέπει να επανεξετάζεται και να αναθεωρείται όταν κρίνεται απαραίτητο λόγω δομικών αλλαγών του εξοπλισμού, του λογισμικού, των κτηρίων και των συνδέσεων δικτύου και διαδικτύου καθώς και σε περιπτώσεις συγχωνεύσεων φορέων με το Δήμο.
- Περιστατικά ασφάλειας πρέπει να αναφέρονται άμεσα μέσω κατάλληλων οδών. Πρέπει να αναλύονται και να αντιμετωπίζονται από το αρμόδιο Τμήμα.
- Εγκατάσταση τείχους προστασίας (hardware ή software) σε όλα τα τερματικά του δικτύου.
- Ρύθμιση των κανόνων πρόσβασης για την επιτρεπόμενη και την απορριπτέα κυκλοφορία με βάση τις ανάγκες του Δήμου Αλμωπίας.
- Υποχρεωτική χρήση πρωτοκόλλων κρυπτογράφησης (TLS/SSL) για όλες τις ευαίσθητες επικοινωνίες και τα δεδομένα που διακινούνται μέσω του δικτύου.
- Εφαρμογή HTTPS για όλες τις διαδικτυακές εφαρμογές και ιστότοπους του οργανισμού για να διασφαλιστεί η ασφάλεια των δεδομένων κατά τη μεταφορά.

Ιστορικό αλλαγών:

Για όλα τα παραπάνω κρατείται ιστορικό αλλαγών-επικαιροποίησης ανά τακτά χρονικά διαστήματα.

Πολιτική Αντι-ικής προστασίας:

Πολιτική:

- Πάντα να γίνεται χρήση του καθιερωμένου και υποστηριζόμενου στα πληροφοριακά συστήματα του Δήμου Αλμωπίας λογισμικού αντιμετώπισης ιών. Όποτε γίνεται διαθέσιμη νεώτερη έκδοσή του αυτή θα πρέπει να εγκαθίσταται αυτόματα και να χρησιμοποιείται. Περιοδικά πρέπει να ενημερώνεται το λογισμικό αντιμετώπισης ιών και οι χρήστες να λαμβάνουν τις προφυλάξεις τους, επειδή εμφανίζονται συνεχώς νέοι ιοί υπολογιστών.
- Η λήψη εισερχόμενου ηλεκτρονικού ταχυδρομείου να γίνεται με την μέγιστη προσοχή λόγω των κινδύνων ασφαλείας που αυτό εμπεριέχει. Το άνοιγμα επισυναπτόμενων αρχείων δεν θα επιτρέπεται εκτός εάν έχει προηγηθεί έλεγχος τους για ύπαρξη ιών ή οποιουδήποτε άλλου είδους επιβλαβούς κώδικα. ΠΟΤΕ να μην ανοίγονται επισυναπτόμενα αρχεία σε ηλεκτρονικό ταχυδρομείο από αναξιόπιστη προέλευση. Αυτά πρέπει να διαγράφονται και αμέσως μετά να γίνεται οριστική διαγραφή τους καθαρίζοντας και την ενδιάμεση περιοχή αποθήκευσης διαγραμμένων αρχείων. Πρέπει να διαγράφονται άχρηστα μηνύματα ηλεκτρονικού ταχυδρομείου και να μην προωθούνται αυτά σε άλλους χρήστες του δικτύου του Δήμου Αλμωπίας. Πρέπει να ενημερώνεται το προσωπικό σχετικά σε ανοικτές συγκεντρώσεις ενημέρωσης του προσωπικού (σεμινάρια).
- Να μην γίνεται κατέβασμα(downloading) αρχείων από ύποπτες πηγές(π.χ. αρχεία άγνωστης μορφής ή συμπιεσμένα αρχεία ή από συνδέσμους ενσωματωμένους στο κείμενο των emails). Η μεταφορά αρχείων-«κατέβασμα» από το διαδίκτυο πρέπει να γίνεται με μεγάλη προσοχή προκειμένου να προστατευθεί ο τοπικός υπολογιστής από επιβλαβές λογισμικό.
- Να μην γίνεται διαμοιρασμός αρχείων σε άλλους χρήστες, δίνοντας τους δικαιώματα τροποποίησης και ανάγνωσης χωρίς αυτό να είναι απολύτως απαραίτητο.
- Όλα τα μαγνητικά μέσα αποθήκευσης θα πρέπει να καταστρέφονται ασφαλώς, εκτός από μαγνητικά μέσα που χρησιμοποιούνται για λήψη αντιγράφων ασφαλείας ή άλλους ειδικούς σκοπούς μεταφοράς αρχείων σε τρίτους.
- Πάντα να ελέγχονται μεταφέρσιμα μέσα αποθήκευσης π.χ. CD-ROM από άγνωστη προέλευση για ύπαρξη ιών.
- Αν κάποιο λογισμικό δεν μπορεί να εκτελεστεί ταυτόχρονα με το λογισμικό αντιμετώπισης ιών, τότε το δεύτερο θα χρησιμοποιηθεί για τον έλεγχο του πρώτου και κατόπιν θα απενεργοποιηθεί προκειμένου να εκτελεστεί η εκάστοτε εφαρμογή.
- Οι εργαζόμενοι να μη χρησιμοποιούν μη εγκεκριμένους screen severs στους φορητούς και προσωπικούς υπολογιστές και στους σταθμούς εργασίας του Δήμου Αλμωπίας. Οι screen severs μπορεί να περιέχουν ιούς ή άλλη μορφή επιβλαβούς λογισμικού προξενώντας βλάβη σε τοπικό επίπεδο ή και σε επίπεδο δικτύου.

Συμμόρφωση Πολιτικής:

Χωρίς εξαίρεση το λογισμικό αντιμετώπισης ιών θα πρέπει να εγκαθίσταται σε όλους τους προσωπικούς υπολογιστές κατά την παράδοση-παραλαβή και να ενημερώνεται τακτικά ανιχνεύοντας εξυπηρετητές, προσωπικούς και φορητούς υπολογιστές. Η πιθανότητα προσβολής από ιούς ελαχιστοποιείται εάν χρησιμοποιείται αποτελεσματικό λογισμικό αντιμετώπισής τους και ενημερώνονται τακτικά οι βιβλιοθήκες απειλών του. Πολλές εταιρείες που παράγουν λογισμικό αντιμετώπισης ιών προσφέρουν τέτοιου είδους ενημέρωση στις ιστοσελίδες τους. Το λογισμικό ανίχνευσης ιών θα πρέπει να προέρχεται από ένα αξιόπιστο προμηθευτή. Επιλογή μη επαρκούς λογισμικού αντιμετώπισης ιών μπορεί να αφήσει τα πληροφοριακά συστήματα του Δήμου Αλμωπίας εκτεθειμένα σε ιούς. Επειδή οι ορισμοί-βιβλιοθήκες του λογισμικού αντιμετώπισης ιών είναι πάντα ενδεικτικές, η επιλογή ενός γνωστού προμηθευτή θα πρέπει να εξεταστεί προσεκτικά, καθώς η ταχύτητα απόκρισής του είναι πολύ σημαντική.

Το σχέδιο αντιμετώπισης περιλαμβάνει τα παρακάτω:

Αρχικά ενημερώνεται το αρμόδιο Τμήμα για την ύπαρξη ύποπτων μηνυμάτων από το λογισμικό προστασίας των ιών. Το αρμόδιο Τμήμα, αξιολογεί τον κίνδυνο, την αιτία και δρομολογεί την επίλυση ανάλογα με την κρισιμότητα, ενημερώνοντας τους χρήστες των συστημάτων για το μέγεθος του προβλήματος και το χρόνο επίλυσής του, καθώς και τις ενέργειες που θα πρέπει να αποφεύγονται κατά τη διάρκεια της επίλυσης.

Πραγματοποιείται τακτικά ανά έτος (ή και πιο τακτικά αν υπάρχει λόγος) καταγραφή ιστορικού αλλαγών στα πληροφορικά συστήματα, καταγραφή των αλλαγών στο λογισμικό και το υλικό δηλαδή, όταν κρίνεται απαραίτητο λόγω δομικών αλλαγών του εξοπλισμού, του λογισμικού, των κτηρίων και των συνδέσεων δικτύου και διαδικτύου καθώς και σε περιπτώσεις συγχωνεύσεων φορέων με το Δήμο.

Θα πρέπει για κάθε αλλαγή θέσης του εξοπλισμού και του λογισμικού να γίνεται έγγραφη ενημέρωση από τους χρήστες, προς το αρμόδιο Τμήμα Προγραμματισμού, Οργάνωσης και Πληροφορικής του Δήμου. Μια φορά κάθε έτος θα γίνεται επιτόπιος έλεγχος επαλήθευσης θέσης, υλικού και λογισμικού. Η αλλαγή θέσης του εξοπλισμού χωρίς επίσημη ενημέρωση του αρμοδίου τμήματος, απαγορεύεται.

Ιστορικό αλλαγών:

Για όλα τα παραπάνω κρατείται ιστορικό αλλαγών-επικαιροποίησης ανά τακτά χρονικά διαστήματα

Πολιτική εγκατάστασης λογισμικού:

Πολιτική:

Η εγκατάσταση νέου λογισμικού, γίνεται μόνο κατόπιν άδειας και εγκατάστασής του από το διαχειριστή του υπολογιστή και του δικτύου και για την προστασία των παραπάνω οι χρήστες ταυτοποιούνται στον υπολογιστή – δίκτυο ως απλοί χρήστες χωρίς δηλαδή να έχουν δικαίωμα εγκατάστασης λογισμικού. Οι επιπλέον διαχειριστές θα ορίζονται με απόφαση δημάρχου. **Τυχόν εξαιρέσεις** στην πολιτική θα είναι μεμονωμένες και καταγεγραμμένες και μόνο όταν το επιτάσσει η απόφαση δημάρχου και η λειτουργικότητα των συστημάτων και διαρκούν για μόνο συγκεκριμένα χρονικά διαστήματα και αίρονται αυτόματα μετά το πέρας αυτών.

Συμμόρφωση Πολιτικής:

Οι χρήστες των τερματικών δεν έχουν δικαιώματα εγκατάστασης εφαρμογών, διότι έχουν οριστεί ως απλοί χρήστες στο domain (δίκτυο). Υπάρχουν εξαιρέσεις κατά τις οποίες σε ορισμένα τερματικά ορισμένοι χρήστες ορίζονται τοπικοί διαχειριστές για συγκεκριμένο χρονικό διάστημα για συγκεκριμένο σκοπό. Κατά αναλογία το ίδιο με τα παραπάνω ισχύει και για τους διαχειριστές όλου του δικτύου.

Ιστορικό αλλαγών:

Για όλα τα παραπάνω κρατείται ιστορικό αλλαγών-επικαιροποίησης ανά τακτά χρονικά διαστήματα.

Πολιτική ασφαλείας διακομιστών (servers):

Πολιτική:

Η πρόσβαση πρέπει να είναι δυνατή μόνο από τους διαχειριστές που έχουν οριστεί χωρίς καμία εξαίρεση.
Όλοι οι διακομιστές θα σχεδιάζονται και θα υλοποιούνται με τεχνικές υψηλής διαθεσιμότητας (high availability) για να διασφαλιστεί η συνεχής λειτουργία των υπηρεσιών. Θα χρησιμοποιούνται τεχνολογίες κατανομής φορτίου για να διαμοιράζεται η εργασία μεταξύ πολλαπλών διακομιστών, αποτρέποντας την υπερφόρτωση και εξασφαλίζοντας την αποδοτικότητα.
Όλοι οι διακομιστές θα είναι συνδεδεμένοι σε σύστημα αδιάλειπτης παροχής ηλεκτρικής ενέργειας (UPS) για την προστασία από διακοπές ρεύματος.

Αντίγραφα Ασφαλείας Αρχείων και Καταγραφών (File/Log Backup). Τακτικά αντίγραφα ασφαλείας θα λαμβάνονται για όλα τα κρίσιμα αρχεία και καταγραφές (logs) των διακομιστών. Τα αντίγραφα ασφαλείας θα αποθηκεύονται με ασφάλεια, τόσο σε τοπικές όσο και σε απομακρυσμένες τοποθεσίες. Τα αντίγραφα ασφαλείας θα είναι κρυπτογραφημένα για να διασφαλιστεί η ακεραιότητα και η εμπιστευτικότητα των δεδομένων.

Ένας δευτερεύων διακομιστής θα είναι εγκατεστημένος και ρυθμισμένος ως εφεδρική λύση για την περίπτωση αποτυχίας του κύριου διακομιστή. Το σύστημα θα έχει τη δυνατότητα αυτόματης εναλλαγής (failover) σε περίπτωση βλάβης του κύριου διακομιστή, εξασφαλίζοντας την ελάχιστη δυνατή διακοπή υπηρεσιών.

Συμμόρφωση Πολιτικής:

Στους διακομιστές (servers) που αφορούν πληροφορίες του συστήματος τα αρχεία εγγράφων (File Servers) πρόσβαση έχει μόνο ο ορισμένος διαχειριστής δικτύου που έχει το αποκλειστικό δικαίωμα πρόσβασης στον server και το δικαίωμα να μην αποκαλύψει πληροφορίες του συστήματος προς οιονδήποτε τρίτο, ειδικά όταν αυτές αφορούν την ασφάλεια του server.
Στους διακομιστές (servers) που αφορούν τις εγκατεστημένες εφαρμογές (Application Servers) η πρόσβαση δίδεται σε εξουσιοδοτημένο υπάλληλο της εταιρίας υποστήριξης των εφαρμογών, ώστε να προχωρήσει στη συντήρηση και αναβάθμιση των εφαρμογών, και το δικαίωμα να μην αποκαλύψει πληροφορίες του συστήματος προς οιονδήποτε τρίτο.

Χρήση τεχνολογιών κατανομής φορτίου (load balancing) για διαμοιρασμό της εργασίας μεταξύ πολλαπλών διακομιστών. Υλοποίηση μηχανισμών αυτόματης ανακατεύθυνσης σε εφεδρικούς διακομιστές σε περίπτωση αποτυχίας (failover). Παρακολούθηση της κατάστασης των διακομιστών και των υπηρεσιών σε πραγματικό χρόνο.

Όλοι οι διακομιστές συνδέονται σε UPS για προστασία από διακοπές ρεύματος. Τα UPS έχουν επαρκή χωρητικότητα και λειτουργούν σωστά μέσω τακτικών ελέγχων.

Έχει καθορισθεί και εφαρμόζεται χρονοδιάγραμμα τακτικών αντιγράφων ασφαλείας για όλα τα κρίσιμα αρχεία και καταγραφές. Τα αντίγραφα ασφαλείας φυλάσσονται σε ασφαλείς τοποθεσίες, τόσο τοπικά όσο και απομακρυσμένα. Συγκεκριμένα αντίγραφα ασφαλείας των εφαρμογών και των αρχείων των χρηστών φυλάσσονται εκτός από εξωτερικό δίσκο στο χώρο του Computer Room, και σε εξωτερικό δίσκο στο χρηματοκιβώτιο του Δήμου όσων αφορά τα αρχεία εφαρμογών. Για τα υπόλοιπα αρχεία των χρηστών αλλά και για τα αρχεία αντιγράφων ασφαλείας προτείνεται η μεταφορά τους με εξωτερικούς δίσκους σε φυλασσόμενο χώρο ευθύνης εκτός της Έδρας του Δήμου. Η μεταφορά θα γίνεται με πρωτόκολλο παράδοσης παραλαβής που θα υπογράφεται κατά την παράδοση και πριν την μεταφορά τους. Για τα παραπάνω θα υπάρξει σχετική απόφαση της Δημοτικής Αρχής που θα ορίζει αναλυτικά τις ενέργειες.

Θα γίνει εγκατάσταση δευτερεύοντος διακομιστή ο οποίος θα είναι ρυθμισμένος να αναλαμβάνει σε περίπτωση αποτυχίας του κύριου διακομιστή. Θα γίνει επίσης υλοποίηση και δοκιμή μηχανισμών αυτόματης εναλλαγής (failover) για την εξασφάλιση ελάχιστης διακοπής των υπηρεσιών.

Ιστορικό αλλαγών:

Για όλα τα παραπάνω κρατείται ιστορικό αλλαγών-επικαιροποίησης ανά τακτά χρονικά διαστήματα.

Πολιτική ασφαλείας σταθμών εργασίας:

Πολιτική:

Η πρόσβαση πρέπει να είναι δυνατή μόνο από τους διαχειριστές που έχουν οριστεί μετά από σχετική ενημέρωση των τοπικών χρηστών και των αντίστοιχων χρηστών των σταθμών εργασίας χωρίς καμία εξαίρεση

Συμμόρφωση Πολιτικής:

Στους σταθμούς εργασίας πρόσβαση έχει μόνο οι ορισμένοι διαχειριστές του σταθμού εργασίας, ώστε να προχωρήσουν στη συντήρηση και αναβάθμιση των εφαρμογών, χωρίς να έχουν πρόσβαση σε αρχεία ή να αλλοιώσουν αρχεία ή φακέλους. Οι χρήστες των σταθμών εργασίας έχουν δικαίωμα χρήσης των εφαρμογών του σταθμού εργασίας και των πόρων του συστήματος, χωρίς να έχουν πρόσβαση σε δυνατότητες αλλαγών που μπορεί να επηρεάσουν τη σωστή λειτουργία των σταθμών εργασίας. Μπορούν να διατηρούν αρχεία σύμφωνα με την κρίση τους στο σταθμό εργασίας και να εφαρμόζουν συστήματα τοπικής κρυπτογράφησης.

Ιστορικό αλλαγών:

Για όλα τα παραπάνω κρατείται ιστορικό αλλαγών-επικαιροποίησης αυτόματα ανά τακτά χρονικά διαστήματα.

- **Πολιτική ασφαλείας σταθμών εργασίας με ευαίσθητα δεδομένα:**

- **Πολιτική:**

Η χρήση των σταθμών εργασίας που χειρίζονται ευαίσθητα δεδομένα, περιλαμβάνει την ισχύουσα πολιτική ασφαλείας που αναφέρθηκε παραπάνω για κάθε σταθμό εργασίας και επιπλέον κάθε δυνατό μέτρο που εξασφαλίζει την μη απώλεια ή διαρροή πληροφοριών σε τρίτους μη εξουσιοδοτημένους χρήστες.

Συμμόρφωση Πολιτικής:

- Όπου κρίνεται απαραίτητο, το έντυπο υλικό και τα υπολογιστικά μέσα θα πρέπει να αποθηκεύονται σε κατάλληλα κλειδωμένο θάλαμο, ειδικά εκτός του ωραρίου εργασίας και ποτέ δεν πρέπει να τοποθετούνται απροστάτευτα (πχ στα γραφεία των υπαλλήλων).
- Κρίσιμη πληροφορία πρέπει να κλειδώνεται σε ασφαλές χώρο.
- Προσωπικοί υπολογιστές, τερματικά και εκτυπωτές δεν θα πρέπει να παραμένουν συνδεδεμένα στο δίκτυο όταν δεν παρακολουθούνται και θα πρέπει να προστατεύονται με συνθηματικά, και άλλα μέτρα ασφάλειας, όταν αυτά δεν χρησιμοποιούνται.
- Η εκτύπωση ευαίσθητης πληροφορίας θα πρέπει να γίνεται μόνο σε συγκεκριμένους εκτυπωτές.
- Ευαίσθητα δεδομένα που κρατούνται στην μνήμη του συστήματος θα πρέπει να ελέγχονται.
- Τα φωτοτυπικά μηχανήματα θα πρέπει να κλειδώνονται (ή γενικά να προστατεύονται από την μη εξουσιοδοτημένη χρήση με κάποιον άλλο τρόπο) εκτός του φυσιολογικού ωραρίου εργασίας.
- Όλοι οι χρήστες των σταθμών εργασίας, προσωπικών υπολογιστών/φορητών υπολογιστών πρέπει να διασφαλίσουν ότι οι οθόνες των υπολογιστών τους είναι καθαρές/κενές όταν δεν χρησιμοποιούνται. Η πληροφορία μπορεί να διαβαστεί από την οθόνη, ειδικά όταν ο υπολογιστής είναι συνδεδεμένος στο δίκτυο ή όταν υπάρχουν έγγραφα ανοικτά προς επεξεργασία.
- Όλοι οι χρήστες των σταθμών εργασίας να παύουν ενεργές συνδέσεις με τους κεντρικούς εξυπηρετητές όταν έχουν τελειώσει, εκτός αν μπορούν να διασφαλισθούν από ένα κατάλληλο μηχανισμό κλειδώματος (για παράδειγμα συνθηματικό προστασίας της οθόνης).

Ιστορικό αλλαγών:

Για όλα τα παραπάνω κρατείται ιστορικό αλλαγών - επικαιροποίησης ανά τακτά χρονικά διαστήματα.

Πολιτική απομακρυσμένης πρόσβασης:

Πολιτική:

Θα πρέπει να παρέχεται άμεση πρόσβαση στους χρήστες μόνο για τις υπηρεσίες για τις οποίες είναι εξουσιοδοτημένοι να χρησιμοποιούν. Αυτό το μέτρο ασφάλειας είναι ιδιαίτερα σημαντικό για δικτυακές συνδέσεις σε ασφαλείς ή κρίσιμες εφαρμογές των πληροφοριακών συστημάτων του Δήμου Αλμωπίας.

Συμμόρφωση Πολιτικής:

- Είναι ευθύνη των εργαζομένων του Δήμου Αλμωπίας, να εξασφαλίζουν ότι δίνουν στη σύνδεση απομακρυσμένης πρόσβασής τους την ίδια προσοχή όπως και οι χρήστες με εσωτερικές συνδέσεις στα πληροφοριακά συστήματα του Δήμου Αλμωπίας.
- Οι απομακρυσμένοι χρήστες των υπηρεσιών θα πρέπει ενημερώνονται για το λογαριασμό τους σε τακτά χρονικά διαστήματα. Αυτό επιτρέπει τον έλεγχο του λογαριασμού τους, αλλά και τον εντοπισμό μιας πιθανής μη εξουσιοδοτημένης χρήσης του.
- Η ασφαλής απομακρυσμένη πρόσβαση πρέπει να ελέγχεται αυστηρά. Ο έλεγχος θα γίνεται με πιστοποίηση κωδικού μίας χρήσης ή δημόσια/ ιδιωτικά κλειδιά με ισχυρά συνθηματικά.

- Οι υπάλληλοι των πληροφοριακών συστημάτων του Δήμου Αλμωπίας και οι συμβαλλόμενοι με δικαιώματα απομακρυσμένης πρόσβασης πρέπει να εξασφαλίζουν ότι ο υπολογιστής ή σταθμός εργασίας τους που ανήκει στα πληροφοριακά συστήματα του Δήμου Αλμωπίας ή είναι ιδιόκτητος και είναι συνδεδεμένος με το δίκτυο των πληροφοριακών συστημάτων του Δήμου Αλμωπίας, δε συνδέεται ταυτόχρονα με οποιοδήποτε άλλο δίκτυο.
- Όλοι οι υπολογιστές που είναι συνδεδεμένοι με το εσωτερικό δίκτυο δεδομένων του Δήμου Αλμωπίας μέσω τεχνολογιών απομακρυσμένης πρόσβασης πρέπει να έχουν το πιο ενημερωμένο λογισμικό καταπολέμησης ιών.
- Ο εξοπλισμός που χρησιμοποιείται για τη σύνδεση με το δίκτυο δεδομένων του Δήμου Αλμωπίας πρέπει να ικανοποιεί τις απαιτήσεις του εξοπλισμού που ανήκει στα πληροφοριακά συστήματα του Δήμου Αλμωπίας για απομακρυσμένη πρόσβαση.

Ιστορικό αλλαγών:

Για όλα τα παραπάνω κρατείται ιστορικό αλλαγών-επικαιροποίησης ανά τακτά χρονικά διαστήματα.

Πολιτική ασφαλείας Δρομολογητή- Μεταγωγέων:

Πολιτική:

Οι δικτυακοί δρομολογητές θα πρέπει να βρίσκονται σε ασφαλές φυσικό περιβάλλον.

Συμμόρφωση Πολιτικής:

- Ο κωδικός πρόσβασης για την τροποποίηση του δρομολογητή θα πρέπει να αλλάζει περιοδικά, σύμφωνα με τις δυνατότητες των υπαλλήλων χρηστών του Δήμου Αλμωπίας, όχι κάτω έξι χαρακτήρες.
- προδιαγραφές της πολιτικής ασφάλειας του Δήμου Αλμωπίας.
- Οι κωδικοί πρόσβασης των χρηστών θα πρέπει να αλλαχτούν από τους αρχικά προκαθορισμένους από τον διαχειριστή.
- Η ακεραιότητα των παραμετροποιήσεων του δρομολογητή θα πρέπει ελέγχεται όταν παραστεί ανάγκη.
- Έμπιστοι δρομολογητές και μεταγωγείς θα πρέπει να ελέγχονται όταν παραστεί ανάγκη. Οι κωδικοί πρόσβασης θα πρέπει να αλλάζουν περιοδικά, σύμφωνα με τις προδιαγραφές της Πολιτικής ασφάλειας του Δήμου Αλμωπίας.

Ιστορικό αλλαγών:

Για όλα τα παραπάνω κρατείται ιστορικό αλλαγών-επικαιροποίησης ανά τακτά χρονικά διαστήματα

Πολιτική αφαιρούμενων αποθηκευτικών μέσων:

Πολιτική:

- Εξουσιοδότηση θα απαιτείται για την απομάκρυνση οποιουδήποτε μεταφέρσιμου αποθηκευτικού μέσου εκτός των εγκαταστάσεων του Δήμου Αλμωπίας, και τέτοιες μετακινήσεις θα πρέπει να καταγράφονται, με πρωτόκολλο παράδοσης-παραλαβής.
- Όλα τα αποθηκευτικά μέσα θα πρέπει να βρίσκονται σε ασφαλές περιβάλλον που θα ικανοποιεί τις προδιαγραφές των κατασκευαστών των αποθηκευτικών μέσων.
- Μόνο εξουσιοδοτημένο προσωπικό θα χρησιμοποιεί μεταφέρσιμα μέσα αποθήκευσης για την μεταφορά δεδομένων εκτός του Δήμου Αλμωπίας. Όλα τα άλλα άτομα θα πρέπει να έχουν ρητή έκτακτη εξουσιοδότηση για να το κάνουν.

- Τα αναλώσιμα των υπολογιστών θα πρέπει να παραγγέλλονται σύμφωνα με τις διαδικασίες που εφαρμόζονται γενικά για το Δήμο Αλμωπίας, ενώ η χρήση τους θα πρέπει να ελέγχεται από την προϊσταμένη εκάστου Τμήματος του Δήμου Αλμωπίας, στην οποία παραδίδονται με πρωτόκολλο παράδοσης-παραλαβής, προκειμένου να αποτραπεί η κλοπή ή μη πρέπουσα χρήση τους.

Συμμόρφωση Πολιτικής:

Γενικά απαγορεύεται η χρήση φορητών αποθηκευτικών μέσων στο Δήμο Αλμωπίας. Προτείνεται αντί αυτών η χρήση εργαλείων δικτύωσης ή ίντερνετ για τη μεταφορά αρχείων. Όπου αυτό δεν είναι δυνατό δίδεται άδεια συγκεκριμένου σκοπού (υποβολή συνημμένων προγραμμάτων, δημιουργία αντιγράφων ασφαλείας, καταγραφής συνομιλιών των αρμοδίων οργάνων κλπ) σε εξουσιοδοτημένους χρήστες για τη χρήση και μεταφορά των εγγράφων των φορητών αποθηκευτικών μέσων, μέχρι την παράδοσή τους στον αρμόδιο για την αποστολή.

Ιστορικό αλλαγών:

Για όλα τα παραπάνω κρατείται ιστορικό αλλαγών-επικαιροποίησης ανά τακτά χρονικά διαστήματα.

Πολιτική απόρριψης συσκευών-υλικού:

Πολιτική:

Τα αποθηκευτικά μέσα πρέπει να απορρίπτονται με ασφάλεια όταν δεν χρειάζονται πλέον. Ευαίσθητη πληροφορία και ειδικά προσωπικά δεδομένα, μπορεί να διαρρεύσει σε εξωτερικά άτομα εξαιτίας της απρόσεκτης απόρριψης αποθηκευτικών μέσων.

Συμμόρφωση Πολιτικής:

- Αποθηκευτικά μέσα που περιέχουν ευαίσθητη πληροφορία πρέπει να φυλάσσονται και να απορρίπτονται ασφαλώς, π.χ. με αποτέφρωση ή θρυμμάτιση, ή άδειασμα από δεδομένα προκειμένου να χρησιμοποιηθούν από άλλη εφαρμογή.
- Αντικείμενα που μπορεί να χρειάζονται ασφαλή απόρριψη, μπορεί είναι τα παρακάτω:
    - έγγραφα
    - φωνητικές ή άλλες εγγραφές
    - εξαγόμενες αναφορές
    - αφαιρούμενοι δίσκοι
    - οπτικά αποθηκευτικά μέσα (όλα τα είδη συμπεριλαμβανομένων και όλων των μέσων διανομής λογισμικού του κατασκευαστή)
    - κώδικας προγραμμάτων
    - δεδομένα δοκιμών
    - τεκμηρίωση συστήματος.

Η απόρριψη ευαίσθητων αντικειμένων πρέπει να καταγράφεται όπου είναι δυνατό, έτσι ώστε να τηρείται ένα αρχείο παρακολούθησης και σύμφωνα με την νομοθεσία για τα προσωπικά δεδομένα.

Όλα τα έγγραφα ευαίσθητης ή εμπιστευτικής φύσης (υποσυστημάτων Υψηλής και Μέσης κρισιμότητας) πρέπει να καταστρέφονται όταν δεν χρειάζονται πλέον. Ο ιδιοκτήτης του εγγράφου πρέπει να εξουσιοδοτεί ή να εκκινεί τη διαδικασία καταστροφής. Όλα τα εκτυπωμένα έγγραφα και αναφορές, ανεπιθύμητες εκτυπώσεις, ιδιαίτερα εμπιστευτικά ή ελεγχόμενα αντίγραφα, πρέπει να απορρίπτονται με ασφάλεια.

Ευαίσθητα δεδομένα που διαγράφονται θα πρέπει να διαγράφονται με ασφαλές τρόπο.

Οποιοσδήποτε υπηρεσία αναλαμβάνει την εξωτερική απόρριψη του πεπαλαιωμένου εξοπλισμού και υλικού πρέπει να επιδεικνύει συμβατότητα με τις πολιτικές ασφάλειας των πληροφοριακών συστημάτων του Δήμου Αλμωπίας.

Η απόρριψη του λογισμικού πρέπει να πραγματοποιείται μόνο όταν το σύστημα δε χρειάζεται πλέον και ότι δε θα απαιτηθεί μελλοντικά η ανάκτηση των συνδεόμενων με αυτό αρχείων δεδομένων τα οποία μπορεί να είναι αρχειοθετημένα.

Ιστορικό αλλαγών:

Για όλα τα παραπάνω κρατείται ιστορικό αλλαγών-επικαιροποίησης ανά τακτά χρονικά διαστήματα.

Η παρούσα απόφαση έλαβε αριθμό **127/2024**

……

Αφού συντάχθηκε και αναγνώσθηκε το πρακτικό αυτό, υπογράφεται ως εξής:

Ο ΠΡΟΕΔΡΟΣ — ΤΑ ΜΕΛΗ

(υπογραφή) — (υπογραφές)

Ακριβές Απόσπασμα

Αριδαία **9-7-2024**

Ο ΠΡΟΕΔΡΟΣ ΔΗΜΟΤΙΚΟΥ ΣΥΜΒΟΥΛΙΟΥ

ΔΟΒΛΕΤΗΣ ΑΝΕΣΤΗΣ