ΕΡΓΟ:

«Ανάπτυξη Συστήματος Συμμόρφωσης με τον Ευρωπαϊκό Κανονισμό 2016/679 (GDPR) για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα»

ΓΕΝΙΚΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

ΔΗΜΟΣ ΒΟΛΟΥ

ΗΜΕΡΟΜΗΝΙΑ

ΕΙΣΑΓΩΓΗ

Η παρακάτω πολιτική ασφάλειας του Δήμου Βόλου αποτελεί αναπόσπαστο μέρος της Πολιτικής Προστασίας Δεδομένων του Δήμου.

Η πολιτική αυτή έχει εκπονηθεί ειδικά για το Τμήμα Ηλεκτρονικής Διακυβέρνησης και Διαφάνειας του Δήμου Βόλου και μπορεί να τροποποιείται όταν υπάρχουν αλλαγές στις διεργασίες του Τμήματος ή αλλαγές στα συστήματά της.

Προϋπόθεση για την τροποποίηση και εφαρμογή της είναι, κατ' αρχήν ο έλεγχος των αλλαγών από τον Υπεύθυνο Προστασίας Δεδομένων του Δήμου και κατόπιν η έγκρισή της από τη Διοίκηση του.

Η πολιτική αποτελείται από τρία (3) διακριτά στοιχεία τα οποία είναι:

Α) Η Γενική πολιτική ασφαλείας

Β) Τα παραρτήματα με τις ειδικές πολιτικές ασφαλείας και

1. Πολιτική Προσβάσεων και Απορρήτου Κωδικών Χρηστών
2. Πολιτική Τήλε-Εργασίας (vpn)
3. Πολιτική Προστασίας Hardware και Δεδομένων
4. Πολιτική Χρήσης Αφαιρούμενων Μέσων
5. Πολιτική Ασφαλείας Δικτύου και Συστημάτων
6. Πολιτική Αντιγράφων Ασφαλείας
7. Πολιτική Καθαρού Γραφείου και Καθαρής Οθόνης
8. Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων
9. Πολιτική Ορθής Χρήσης Σταθμών Εργασίας
10. Πολιτική Ασφαλούς Μεταφοράς Πληροφοριών
11. Πολιτική Ασφαλούς Αποστολής Μηνυμάτων Ηλεκτρονικού Ταχυδρομείου (e-mail)
12. Πολιτική B.Y.O.D.

13. Πολιτική Κατηγοριοποίησης Συστημάτων

14. Πολιτική Τηλεδιασκέψεων

Γ) Τα συνημμένα έγγραφα , όπου αυτά υφίστανται, τα οποία συνοδεύουν συγκεκριμένες ειδικές πολιτικές ασφάλειας.

ΥΠΕΥΘΥΝΟΣ ΠΟΛΙΤΙΚΗΣ	ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ	ΕΓΚΡΙΣΗ Δ.Σ.
ΒΑΜΒΑΚΑΣ ΜΙΧΑΗΛ	AQS Advanced Quality Services Ltd.	ΧΧ

Ημερομηνία Έκδοσης
ΧΧ/ΨΨ/ΩΩΩΩ

ΠΙΝΑΚΑΣ ΑΝΑΘΕΩΡΗΣΕΩΝ

ΑΡΙΘΜΟΣ ΑΝΑΘΕΩΡΗΣΗΣ	ΗΜΕΡΟΜΗΝΙΑ	ΠΕΡΙΓΡΑΦΗ ΤΡΟΠΟΠΟΙΗΣΗΣ

Περιεχόμενα

1 Α. ΓΕΝΙΚΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ 10

1.1 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ 10

1.2 ΣΥΝΤΜΗΣΕΙΣ 10

1.3 ΕΦΑΡΜΟΓΗ 10

1.4 ΝΟΜΙΚΟ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ 10

1.5 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 11

1.6 ΣΚΟΠΟΣ 11

1.7 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ 12

1.8 ΑΡΜΟΔΙΟΤΗΤΕΣ 13

1.8.1 Αρμοδιότητες διοίκησης 13

1.8.2 Αρμοδιότητες του Υπεύθυνου Προστασίας Δεδομένων 13

1.8.3 Αρμοδιότητες Ομάδας Διαχείρισης Ασφάλειας Δεδομένων 15

1.8.4 Αρμοδιότητες Προϊσταμένων Διευθύνσεων 16

1.8.5 Αρμοδιότητες προσωπικού 16

1.9 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ 16

1.10 ΑΡΧΕΙΑ 17

Β. ΠΑΡΑΡΤΗΜΑΤΑ 18

ΠΑΡΑΡΤΗΜΑ Ι 19

ΕΙΔΙΚΕΣ ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ 19

1. ΠΟΛΙΤΙΚΗ ΠΡΟΣΒΑΣΕΩΝ ΚΑΙ ΑΠΟΡΡΗΤΟΥ ΚΩΔΙΚΩΝ 19

1.1 ΣΚΟΠΟΣ 19

1.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 19

1.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 19

1.4 ΔΙΚΑΙΩΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΡΟΣΒΑΣΕΩΝ 20

1.4.1 Πρόσβαση στο λειτουργικό σύστημα και στο εσωτερικό δίκτυο 22

1.4.2 Πρόσβαση στους file Servers 22

1.4.3 Πρόσβαση σε ηλεκτρονικό ταχυδρομείο (email) 23

1.4.4 Πρόσβαση στο διαδίκτυο 24

1.4.5 Απομακρυσμένη πρόσβαση στο εσωτερικό δίκτυο (VPN) 24

1.4.6 Πρόσβαση σε Εφαρμογές (ERP, κλπ.) 24

1.5 ΔΙΑΧΕΙΡΙΣΗ ΤΩΝ ΚΩΔΙΚΩΝ 25

1.6 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ 26

1.7 ΑΡΧΕΙΑ 26

2 ΠΟΛΙΤΙΚΗ ΤΗΛΕΡΓΑΣΙΑΣ (VPN) 26

2.1 ΣΚΟΠΟΣ 26

2.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 27

2.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 27
2.4 ΧΡΗΣΗ ΣΥΣΚΕΥΩΝ 27
2.4.1 Ρυθμίσεις συσκευής 27
2.4.2 Ελάχιστα κριτήρια ασφάλειας Η/Υ 27
2.4.3 Ρυθμίσεις ασφαλείας vpn σύνδεσης 28
2.5 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ 28
3 ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ HARDWARE ΚΑΙ ΔΕΔΟΜΕΝΩΝ 28
3.1 ΣΚΟΠΟΣ 28
3.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 29
3.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 29
3.4 ΠΕΡΙΓΡΑΦΗ 29
3.4.1 Φυσική προστασία Hardware 29
3.4.2 Datacenters 29
3.4.3 Computer Room 30
3.4.4 Διόρθωση/επισκευή βλαβών 30
3.5 ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ 31
3.5.1 Δεδομένα σε Servers 31
3.6 ΠΡΟΣΤΑΣΙΑ & ΑΠΟΤΡΟΠΗ ΙΩΝ 32
3.6.1 Εγκατάσταση και λειτουργία Firewall 32
3.7 ΣΕ DESKTOP PC'S & LAPTOPS 32
3.7.1 Firewall 32
3.7.2 Εγκατάσταση και λειτουργία antivirus & antispam 32
3.7.3 Καθορισμός δικαιωμάτων πρόσβασης 33
3.8 ΚΡΥΠΤΟΓΡΑΦΗΣΗ 33
3.9 ΣΥΝΗΜΜΕΝΑ ΈΝΤΥΠΑ 33
4 ΠΟΛΙΤΙΚΗ ΧΡΗΣΗΣ ΑΦΑΙΡΟΥΜΕΝΩΝ ΜΕΣΩΝ 34
4.1 ΣΚΟΠΟΣ 34
4.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 34
4.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 34
4.4 ΠΕΡΙΓΡΑΦΗ 34
4.4.1 Χρήση Laptops 34
4.4.2 Χρήση Κινητών Τηλεφώνων 34
4.4.3 Χρήση Αφαιρούμενων Δίσκων και μέσων (εξωτερικοί δίσκοι, CDs, DVDs, USB flash disks κλπ) 35
5 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ 35
5.1 ΣΚΟΠΟΣ 35
5.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 36
5.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 37

5.4 ΠΕΡΙΓΡΑΦΗ 37
5.4.1 Ασφάλεια Περιμέτρου 37
5.4.2 Πολιτική ασφάλειας συστημάτων 38
5.4.3 Παρακολούθηση (Monitoring) και Έλεγχος 39
5.4.4 Χρήση VPN – Remote Access 40
*5.4.5 Επιτρεπόμενη και μη χρήση των συστημάτων ..... **Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.***
5.4.6 Πολιτική ασφάλειας fileserver 40
5.4.7 Ενημέρωση λογισμικού 41
5.5 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ 41
5.6 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ 41
6 ΠΟΛΙΤΙΚΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ 42
6.1 ΣΚΟΠΟΣ 42
6.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 42
6.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 42
6.4 ΔΗΜΙΟΥΡΓΙΑ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ 42
6.5 ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ 43
6.6 ΑΝΑΚΤΗΣΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ 43
6.7 ΈΛΕΓΧΟΣ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ 44
6.8 ΑΡΧΕΙΑ 44
7 ΠΟΛΙΤΙΚΗ ΚΑΘΑΡΟΥ ΓΡΑΦΕΙΟΥ ΚΑΙ ΚΑΘΑΡΗΣ ΟΘΟΝΗΣ 44
7.1 ΣΚΟΠΟΣ 44
7.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 45
7.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 45
7.4 ΠΕΡΙΓΡΑΦΗ 45
8 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΕΛΕΓΧΩΝ 46
8.1 ΣΚΟΠΟΣ 46
8.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 46
8.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 46
8.4 ΠΕΡΙΓΡΑΦΗ 46
8.5 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ 47
8.6 ΑΡΧΕΙΑ 47
9 ΠΟΛΙΤΙΚΗ ΟΡΘΗΣ ΧΡΗΣΗΣ ΣΤΑΘΜΩΝ ΕΡΓΑΣΙΑΣ 47
9.1 ΣΚΟΠΟΣ 47
9.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 47
9.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 48
9.4 ΠΕΡΙΓΡΑΦΗ 48
9.4.1 Αποδεκτή Χρήση Σταθμών Εργασίας και Πρόσβασης στο Διαδίκτυο 48

9.4.2 Πεδίο Εφαρμογής 48
9.4.3 Υπεύθυνος Εφαρμογής της Πολιτικής 48
9.4.4 Αποδεκτή Χρήση Σταθμών Εργασίας και Πρόσβασης στο Διαδίκτυο 48
9.4.5 Μη αποδεκτή χρήση συστημάτων 48
9.4.6 Πρόσβαση Διαδυκτιακών Τόπων 50
9.5 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ 50
9.6 ΑΡΧΕΙΑ 50
10 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΟΥΣ ΜΕΤΑΦΟΡΑΣ ΠΛΗΡΟΦΟΡΙΩΝ 50
10.1 ΓΕΝΙΚΑ 50
10.2 ΣΚΟΠΟΣ 51
10.3 ΕΞΑΙΡΕΣΕΙΣ 51
10.4 ΟΡΙΣΜΟΙ 52
10.5 ΡΟΛΟΙ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ 52
10.5.1 Αποστολέας 52
10.5.2 Υπεύθυνος Ασφάλειας 52
10.5.3 Προϊστάμενοι τμημάτων 53
10.5.4 Υπάλληλοι 53
10.6 ΑΡΜΟΔΙΟΤΗΤΕΣ ΑΠΟΣΤΟΛΕΑ 53
10.7 ΝΟΜΙΜΟΤΗΤΑ ΚΑΙ ΑΝΑΓΚΑΙΟΤΗΤΑ ΜΕΤΑΦΟΡΑΣ 53
10.8 ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ 54
10.9 ΕΜΠΙΣΤΕΥΤΙΚΑ ΔΕΔΟΜΕΝΑ 54
10.10 ΑΠΑΙΤΗΣΕΙΣ ΜΕΤΑΦΟΡΑΣ ΠΡΟΣΩΠΙΚΩΝ Η ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΔΕΔΟΜΕΝΩΝ 55
10.11 ΗΛΕΚΤΡΟΝΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ 55
10.12 ΔΙΚΤΥΑΚΗ ΜΕΤΑΦΟΡΑ (FTP, SECUREFTP , VPN) 55
10.13 ΑΦΑΙΡΟΥΜΕΝΟ ΜΕΣΟ (CD, USB ΔΙΣΚΟΣ, ΚΑΡΤΑ ΜΝΗΜΗΣ ΚΛΠ.) 56
10.14 ΜΕΤΑΔΟΣΗ FAX 56
10.15 ΤΑΧΥΔΡΟΜΙΚΗ Η ΜΕ COURIER ΑΠΟΣΤΟΛΗ 56
10.16 ΤΗΛΕΦΩΝΙΚΗ ΜΕΤΑΔΟΣΗ 57
10.17 SMS, ΜΗΝΥΜΑΤΑ ΚΟΙΝΩΝΙΚΩΝ ΔΙΚΤΥΩΝ, ΕΦΑΡΜΟΓΕΣ ΆΜΕΣΩΝ ΜΗΝΥΜΑΤΩΝ (INSTANT MESSAGING) . 57
10.18 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ 57
10.19 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ 58
10.20 ΑΡΧΕΙΑ 58
11 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΟΥΣ ΑΠΟΣΤΟΛΗΣ E-MAIL 58
11.1 ΣΚΟΠΟΣ 58
11.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 58
11.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 59
11.4 ΠΕΡΙΓΡΑΦΗ 59
11.4.1 Παραδοχές 59

11.5 ΚΑΝΟΝΕΣ ΑΠΟΣΤΟΛΗΣ 59
11.6 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ 59
11.7 ΧΡΗΣΙΜΟΠΟΙΟΥΜΕΝΑ ΕΝΤΥΠΑ 60
11.8 ΑΡΧΕΙΑ 60
12 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ B.Y.O.D. (BRING YOUR OWN DEVICE) 60
12.1 ΣΚΟΠΟΣ 60
12.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 60
12.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 60
12.4 ΠΕΡΙΓΡΑΦΗ 61
12.4.1 Χρήση Συσκευών 61
12.5 ΑΣΦΑΛΕΙΑ ΣΥΣΚΕΥΗΣ 62
12.5.1 Ρυθμίσεις συσκευής 62
12.5.2 Ελάχιστα κριτήρια ασφάλειας 62
12.5.3 Εγκεκριμένα Προγράμματα 62
12.6 ΤΕΧΝΙΚΗ ΥΠΟΣΤΗΡΙΞΗ 63
12.7 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ 63
12.8 ΑΡΧΕΙΑ 63
13 ΠΟΛΙΤΙΚΗ ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗΣ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΕΔΟΜΕΝΩΝ 64
14 ΠΟΛΙΤΙΚΗ ΤΗΛΕΔΙΑΣΚΕΨΕΩΝ 64
14.1 ΣΚΟΠΟΣ 64
14.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ 64
14.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 65
14.4 ΠΕΡΙΓΡΑΦΗ 65
14.4.1 Τηλε-εργασία – Χρήση Συσκευών 65
14.4.2 Ρυθμίσεις Ασφάλειας Συσκευής 65
14.4.3 Ρυθμίσεις Ασφαλείας Σύνδεσης 66
14.5 ΤΗΛΕ-ΕΡΓΑΣΙΑ – ΥΠΕΥΘΥΝΟΤΗΤΕΣ 66
14.5.1 Τμήμα Πληροφορικής 66
14.5.2 Χρήστες Τηλε-εργασίας 67
14.6 ΤΗΛΕΔΙΑΣΚΕΨΕΙΣ – ΑΣΦΑΛΕΙΑ ΣΥΝΔΕΣΗΣ 68
14.7 ΑΣΦΑΛΕΙΑ ΕΦΑΡΜΟΓΩΝ ΤΗΛΕΔΙΑΣΚΕΨΗΣ 69
14.8 ΕΦΑΡΜΟΓΕΣ ΤΗΛΕΔΙΑΣΚΕΨΗΣ 69
14.9 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ 70
14.10 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ 70
14.11 ΑΡΧΕΙΑ 70
ΠΑΡΑΤΗΜΑ ΙΙ 70
ΛΙΣΤΑ ΠΡΟΓΡΑΜΜΑΤΩΝ 70
1 ΕΓΚΕΚΡΙΜΕΝΑ 70

2 ΠΡΟΣΘΕΤΑ 71

1 Α. Γενική Πολιτική Ασφάλειας

1.1 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

Το Σύστημα Διαχείρισης Ασφάλειας Δεδομένων (ΣΔΑΔ) εφαρμόζεται από όλες τις Διευθύνσεις / Τμήματα / Γραφεία του Δήμου.

1.2 ΣΥΝΤΜΗΣΕΙΣ

ΓεΠΑΔ: Γενική Πολιτική Ασφάλειας Δεδομένων (το παρόν έγγραφο)

ΥΠΔ: Υπεύθυνος Προστασίας Δεδομένων

ΙΤ: Υπεύθυνος Διαχείρισης Πληροφοριακών Συστημάτων και Δικτύων

1.3 ΕΦΑΡΜΟΓΗ

Η ΓεΠΑΔ εφαρμόζεται από όλο το προσωπικό του Δήμου που εμπλέκεται στην εκτέλεση των Υπηρεσιών, καθώς επίσης και στο χρησιμοποιούμενο εξοπλισμό, αλλά και στις εγκαταστάσεις που χρησιμοποιεί ο Δήμος στα πλαίσια εκτέλεσης των Υπηρεσιών αυτών, συμπεριλαμβανομένων των όποιων πρόσθετων όρων των σχετικών συμβάσεων.

1.4 ΝΟΜΙΚΟ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ

Το Νομικό και Κανονιστικό πλαίσιο προσδιορίζεται από:

- Ν. 3463/2006 - ΦΕΚ Α’ 114/30.6.2006 – Άρθρο 75 (Κώδικας Δήμων και Κοινοτήτων)
- Νόμος 4624/2019 (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις".)
- Απόφαση ΑΔΑΕ 165/2011 (Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών.

- Ν.2121 ΦΕΚ 25 Α / 04-03-1993 Νόμος περί προστασίας και αποφυγής κλοπής πνευματικής ιδιοκτησίας.
- Ν.3741/2006 Νόμος για την προστασία δεδομένων προσωπικού χαρακτήρα και ιδιωτικής ζωής στον τομέα των ηλεκτρονικών.
- Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
- Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)
- Οδηγία (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Σεπτεμβρίου 2015, για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών.

Σημείωση: Ο Δήμος δεσμεύεται όπως δεν αποδεχτεί οιονδήποτε συμβατικό όρο που παραβιάζει το ανωτέρω Νομικό και Κανονιστικό πλαίσιο.

1.5 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- Όλα τα στελέχη
- Όλοι οι υπάλληλοι

1.6 ΣΚΟΠΟΣ

Ο Δήμος επιδιώκει την παροχή των Υπηρεσιών σύμφωνα με το ισχύον Νομικό και Κανονιστικό πλαίσιο και τις λοιπές συμβατικές υποχρεώσεις του, με τρόπο που να προστατεύονται τα πληροφοριακά δεδομένα και ιδιαίτερα τα προσωπικά από εκούσια ή ακούσια κλοπή, καταστροφή, ή χρήση κατά παράβαση των Νόμων και των Κανονιστικών Διατάξεων.

Ο σκοπός της ασφάλειας των προσωπικών δεδομένων είναι να διασφαλίσει την επιχειρησιακή συνέχεια του Δήμου και να ελαχιστοποιήσει τους κινδύνους που επαπειλούν τα δεδομένα,

αποφεύγοντας περιστατικά ασφαλείας και μειώνοντας τις επιπτώσεις που μπορεί να έχουν τα περιστατικά αυτά.

1.7 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

Στόχος της παρούσας πολιτικής είναι να προστατέψει τα Πληροφοριακά Δεδομένα του Δήμου από όλες τις εσωτερικές, εξωτερικές, εκούσιες ή ακούσιες απειλές. Για την επίτευξη του στόχου αυτού, εκτός της παρούσης γενικής πολιτικής έχουν εκπονηθεί και ειδικές πολιτικές ασφαλείας όπως φαίνονται στα παραρτήματα Α1 – Α13 του παρόντος εγγράφου και αποτελούν αναπόσπαστο μέρος αυτού.

Οι επιμέρους στόχοι του Δήμου σχετικά με την Ασφάλεια των Δεδομένων είναι:

- Τα Πληροφοριακά Δεδομένα να είναι προστατευμένα από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση.
- Να διασφαλίζεται η εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και η διατήρηση των Πληροφοριακών Δεδομένων, όπως νομίμως προβλέπεται.
- Να τηρούνται πάντα οι αρχές της νομιμότητας, αντικειμενικότητας και διαφάνειας κατά την επεξεργασία των Πληροφοριακών Δεδομένων.
- Τα Πληροφοριακά Δεδομένα να συλλέγονται μόνο για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς.
- Τα Πληροφοριακά Δεδομένα να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.
- Να διασφαλίζεται η τήρηση των νομοκανονιστικών απαιτήσεων.
- Να παρέχεται εκπαίδευση πάνω στην Ασφάλεια των Δεδομένων για όλο το προσωπικό.
- Όλα τα πραγματικά ή καθ' υποψία περιστατικά ασφαλείας να αναφέρονται στον ΥΠΔ και να διερευνώνται πλήρως.

Για την επίτευξη των παραπάνω στόχων έχουν αναπτυχθεί και εφαρμόζονται επιμέρους Τεχνικά Μέτρα, Πολιτικές Ασφαλείας και Διαδικασίες, όπου περιγράφονται και όλες οι σχετικές αρμοδιότητες του προσωπικού και οι οποίες διασφαλίζουν και αποδεικνύουν ότι η διαχείριση των πληροφοριακών δεδομένων διενεργείται σύμφωνα με το Νομοκανονιστικό Πλαίσιο.

Τα εν λόγω Μέτρα, Πολιτικές και Διαδικασίες επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο, όπως για παράδειγμα μετά από εκτεταμένες αλλαγές στα πληροφοριακά

συστήματα, βασικές αλλαγές στα προγράμματα (software), κλπ., και κατ' ελάχιστο ανά έτος. Υπεύθυνος για την επικαιροποίηση είναι ο ΥΠΔ, σε συνεργασία με τους Προϊσταμένους των Διευθύνσεων.

Όλο το προσωπικό και οι εξωτερικοί συνεργάτες (όταν αυτό απαιτείται) είναι υποχρεωμένοι να εφαρμόζουν τις Πολιτικές Ασφαλείας που διέπουν τη λειτουργία του Δήμου και εμπίπτουν στο πεδίο των δραστηριοτήτων τους.

Η Διοίκηση δεσμεύεται για την παροχή όλων των απαραίτητων πόρων και μέσων για την εφαρμογή της παρούσας και των επιμέρους Πολιτικών Ασφαλείας.

1.8 ΑΡΜΟΔΙΟΤΗΤΕΣ

1.8.1 Αρμοδιότητες διοίκησης

Οι βασικές αρμοδιότητες της Διοίκησης σε σχέση με τη διαχείριση της Ασφάλειας Δεδομένων στον Δήμο είναι:

- Η διαμόρφωση της πολιτικής του Δήμου σε σχέση με την Ασφάλεια Δεδομένων.
- Η έγκριση και η ανασκόπηση των Πολιτικών Ασφαλείας.
- Η έγκριση του Πλάνου Εκτίμησης Επικινδυνότητας και των Σχεδίων Διαχείρισης Εκτάκτων Αναγκών.
- Η διασφάλιση των πόρων που απαιτούνται για την αποτελεσματική εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Δεδομένων.
- Η δημιουργία των απαραίτητων συνθηκών στον Δήμο για την προώθηση της κατανόησης και εμπέδωσης από το προσωπικό του ρόλου και των ευθυνών του που συνδέονται με την Ασφάλεια Δεδομένων.
- Η μέριμνα για τη συνεχή βελτίωση του Συστήματος Διαχείρισης Ασφάλειας των Δεδομένων.

1.8.2 Αρμοδιότητες του Υπεύθυνου Προστασίας Δεδομένων

Εκπρόσωπος της Διοίκησης σε θέματα Ασφάλειας Δεδομένων είναι ο Υπεύθυνος Προστασίας Δεδομένων. Ο ΥΠΔ ορίζεται με απόφαση της Διοίκησης και επιπλέον των άλλων καθηκόντων, έχει τις υπευθυνότητες που αναφέρονται στη συνέχεια:

- Διαμορφώνει την αρχιτεκτονική του οικοδομήματος προστασίας (by design & by default).

- Καταγράφει τις διαδικασίες συλλογής, αποθήκευσης, μεταβίβασης και επεξεργασίας των προσωπικών δεδομένων.
- Ενημερώνει και συμβουλεύει τη Διοίκηση και το προσωπικό για τις υποχρεώσεις του που απορρέουν από το Νομοκανονιστικό Πλαίσιο σχετικά με την προστασία δεδομένων.
- Παρακολουθεί τη συμμόρφωση με το Νομοκανονιστικό Πλαίσιο σχετικά με την προστασία δεδομένων και με τις πολιτικές του Δήμου σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων.
- Μεριμνά για τη ευαισθητοποίηση και εκπαίδευση του προσωπικού του Δήμου σε θέματα Ασφάλειας Δεδομένων, Πολιτικών και Διαδικασιών και απαιτήσεων Νομοκανονιστικού Πλαισίου.
- Οργανώνει, συντάσσει εκθέσεις αποτίμησης κινδύνου (Privacy Impact Assessments).
- Παρέχει συμβουλές, όταν ζητείται, όσον αφορά την Εκτίμηση Αντικτύπου και Επικινδυνότητας, σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησής της.
- Συνεργάζεται με εποπτικές αρχές και επικοινωνεί με την εποπτικές αρχές για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της διαβούλευσης.
- Σχεδιάζει εσωτερικές διαδικασίες & εργαλεία συμμόρφωσης.
- Συνεργάζεται με τη Διοίκηση και τις Διευθύνσεις, για την ανάπτυξη Πολιτικών Ασφαλείας, διαδικασιών και πρότυπων μεθόδων, σύμφωνα με την Γενική Πολιτική Ασφάλειας Δεδομένων του Δήμου.
- Μέριμνα για την εφαρμογή, διατήρηση και παρακολούθηση των Πολιτικών Ασφάλειας, ώστε να διασφαλίζεται η τήρηση των νομοκανονιστικών απαιτήσεων, της εκάστοτε ισχύουσας νομοθεσίας και των απαιτήσεων των προτύπων.
- Ενημερώνει τη Διοίκηση για την επίδοση και βελτίωση των Πολιτικών Ασφάλειας.
- Ελέγχει τον κατάλογο πληροφοριακών στοιχείων του Δήμου και τη διαβάθμιση της σπουδαιότητάς τους (ΕΠ.05.01 ΜΗΤΡΩΟ ΣΥΣΚΕΥΩΝ), σε συνεργασία με τα αρμόδια επιχειρησιακά στελέχη κάθε Διεύθυνσης.
- Συνεργάζεται με τη Διοίκηση και την Ομάδα Διαχείρισης Ασφάλειας Δεδομένων για τον καθορισμό των απαραίτητων ελέγχων για την αντιμετώπιση των κινδύνων.

- Σχεδιάζει διαδικασίες αντιμετώπισης κινδύνων / παραβιάσεων / λοιπών περιστατικών και ενημέρωσης.
- Παρακολουθεί και αναφέρει στη Διοίκηση οποιοδήποτε περιστατικό ασφαλείας και ενεργοποιεί το αντίστοιχο σχέδιο και στρατηγική για την αντιμετώπιση και την αποφυγή επανεμφάνισής του.
- Λογοδοτεί απέναντι στα υποκείμενα επεξεργασίας εάν χρειαστεί.
- Παρακολουθεί την αποτελεσματικότητα των ελέγχων που εφαρμόζονται για την αντιμετώπιση των κινδύνων και αναφέρει σχετικά στη Διοίκηση.

Ο ΥΠΔ αναφέρεται απευθείας στην Διοίκηση για όλα τα θέματα σχετικά με την Ασφάλεια Δεδομένων και είναι εξουσιοδοτημένος να ενεργεί για λογαριασμό της σχετικά με αυτά.

1.8.3 Αρμοδιότητες Ομάδας Διαχείρισης Ασφάλειας Δεδομένων

Ως μέλη της Ομάδας Διαχείρισης Ασφάλειας Δεδομένων θα πρέπει να ορίζονται:

- Ένας Υπεύθυνος Διαχειριστής Ασφάλειας (ΙΤ)
- Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ)
- Προϊστάμενος Διεύθυνσης

Οι βασικές αρμοδιότητες της Ομάδας Διαχείρισης Ασφάλειας Δεδομένων είναι:

- Η εξέταση των δραστηριοτήτων του Δήμου που εμπίπτουν στο πεδίο εφαρμογής του ΣΔΑΔ και ο εντοπισμός των εμπλεκομένων πληροφοριακών περιουσιακών στοιχείων και των κινδύνων που τα απειλούν.
- Η εκτίμηση αντίκτυπου και αξιολόγηση της επικινδυνότητας των εντοπισθέντων κινδύνων.
- Η εξέταση, οι προτάσεις και η καταγραφή μέτρων ελέγχου για την αντιμετώπιση των κινδύνων.
- Η περιοδική ανασκόπηση της αποτελεσματικότητας των πλάνων διαχείρισης των κινδύνων.
- Ο εντοπισμός των περιπτώσεων κατάστασης εκτάκτου ανάγκης και συντονισμών των ενεργειών για την κατάρτιση και έγκριση σχεδίων εκτάκτου ανάγκης.

- Η αντιμετώπιση περιστατικών Ασφάλειας Δεδομένων.

1.8.4 Αρμοδιότητες Προϊσταμένων Διευθύνσεων

Οι βασικές αρμοδιότητες των Προϊσταμένων των Διευθύνσεων του Δήμου σε σχέση με τη διαχείριση της Ασφάλειας Δεδομένων είναι:

- Η συμμετοχή στον εντοπισμό, την εκτίμηση και το σχεδιασμό της διαχείρισης των κινδύνων που σχετίζονται με τα πληροφοριακά αγαθά που διαχειρίζεται η Διεύθυνση τους.
- Η επίβλεψη της τήρησης των Πολιτικών Ασφαλείας από τα στελέχη της Διεύθυνσής τους.
- Η ενεργός συμμετοχή στην ανασκόπηση σχετικών περιστατικών ασφαλείας, ώστε να διερευνηθούν οι αιτίες τους και να σχεδιαστούν οι απαραίτητες διορθωτικές ενέργειες.
- Ο εντοπισμός σημαντικών αλλαγών και τάσεων που μπορεί να επηρεάσουν τις πρακτικές για την Ασφάλεια της πληροφορίας στο χώρο ευθύνης τους και η συνεργασία με τον ΥΠΔ και τη Διοίκηση για την προσαρμογή στις νέες συνθήκες.

1.8.5 Αρμοδιότητες προσωπικού

Οι βασικές αρμοδιότητες του εμπλεκόμενου στο Σύστημα Διαχείρισης Ασφάλειας Δεδομένων προσωπικού σε σχέση με τη διαχείριση της Ασφάλειας Δεδομένων του Δήμου είναι:

- Η εφαρμογή των Πολιτικών Ασφαλείας, των σχετικών διαδικασιών και οδηγιών εργασίας που εμπίπτουν κατά την εκτέλεση της εργασίας του.
- Η άμεση αναφορά στον ΥΠΔ οποιουδήποτε περιστατικού ασφαλείας εμπίπτει στην αντίληψή του.

1.9 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ

Οργανόγραμμα Δήμου

1.10 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
Οργανόγραμμα Δήμου	Ηλεκτρονική	Επ' αόριστο	ΥΠΔ

Β. ΠΑΡΑΡΤΗΜΑΤΑ

Ι. Ειδικές Πολιτικές Ασφάλειας

1. Πολιτική Προσβάσεων και Απορρήτου Κωδικών Χρηστών
2. Πολιτική Τήλε-Εργασίας (vpn)
3. Πολιτική Προστασίας Hardware και Δεδομένων
4. Πολιτική Χρήσης Αφαιρούμενων Μέσων
5. Πολιτική Ασφαλείας Δικτύου και Συστημάτων
6. Πολιτική Αντιγράφων Ασφαλείας
7. Πολιτική Καθαρού Γραφείου και Καθαρής Οθόνης
8. Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων
9. Πολιτική Ορθής Χρήσης Σταθμών Εργασίας
10. Πολιτική Ασφαλούς Μεταφοράς Πληροφοριών
11. Πολιτική Ασφαλούς Αποστολής Μηνυμάτων Ηλεκτρονικού Ταχυδρομείου (e-mail)
12. Πολιτική B.Y.O.D.
13. Πολιτική Κατηγοριοποίησης Συστημάτων
14. Πολιτική Τηλεδιασκέψεων

ΙΙ. Λίστα Προγραμμάτων

1. Εγκεκριμένα

2. Πρόσθετα

ΠΑΡΑΡΤΗΜΑ Ι

Ειδικές Πολιτικές Ασφάλειας Δεδομένων

1. Πολιτική Προσβάσεων και Απορρήτου Κωδικών Χρηστών

1.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγράψει τη μεθοδολογία που ακολουθείται στη χρήση των κωδικών από τους χρήστες τους. Ιδιαίτερα περιγράφονται οι μέθοδοι που εφαρμόζονται για τη διαχείριση αυτών των κωδικών στον Δήμο. Επίσης περιγράφονται οι λογικές προσβάσεις που υπάρχουν στον Δήμο και ο τρόπος πρόσβασης των υπηρεσιών αυτών από τους χρήστες.

1.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται για τους κωδικούς πρόσβασης όλων των χρηστών στους προσωπικούς σταθμούς εργασίας, στο εσωτερικό δίκτυο του Δήμου, για την πρόσβαση στο διαδίκτυο και την ειδική πρόσβαση σε εξειδικευμένες εφαρμογές.

Η ανασκόπηση των δικαιωμάτων των χρηστών που απορρέουν από την παρούσα πολιτική ορίζεται ότι θα εκτελείται σε ετήσια βάση.

1.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Υπεύθυνος Προστασίας Δεδομένων
- Υπεύθυνος Διαχείρισης Πληροφοριακών Συστημάτων και Δικτύων (IT)
- Χρήστες συστημάτων
- Εξωτερικοί Συνεργάτες

1.4 Δικαιώματα ηλεκτρονικών προσβάσεων

Τα δικαιώματα ηλεκτρονικών προσβάσεων στον Δήμο είναι διαφόρων ειδών και απαριθμούνται ακολούθως:

1. Πρόσβαση στο λειτουργικό σύστημα (π.χ. windows) στους σταθμούς εργασίας
2. Πρόσβαση στους file servers (domain users)
3. Πρόσβαση σε υπηρεσία e-mail
4. Πρόσβαση σε ειδικές εφαρμογές:

   ΕΣΩΤΕΡΙΚΕΣ ΕΦΑΡΜΟΓΕΣ (έχουν κατασκευαστεί από Υπαλ. του τμήματος Ηλεκτρ. Διακ. Και διαφάνειας)

   a. **Ηλεκτρονική Εφαρμογή Διαχείρισης έργων (ΒΑΜΒΑΚΑΣ ΜΙΧΑΛΗΣ)**
   b. **Γραφείο Προσωπικού /Παρουσιολόγιο (ΒΑΜΒΑΚΑΣ ΜΙΧΑΛΗΣ)**
   c. **Μητρώο Παγίων (ΒΑΜΒΑΚΑΣ ΜΙΧΑΛΗΣ)**
   d. **Network (ΒΑΜΒΑΚΑΣ ΜΙΧΑΛΗΣ)**
   e. **ΚΑΠΗ (ΒΑΜΒΑΚΑΣ ΜΙΧΑΛΗΣ)**
   f. **Ευρετήριο Τηλεφώνων (ΒΑΜΒΑΚΑΣ ΜΙΧΑΛΗΣ)**
   g. **Διαχείριση Στόλου (ΒΑΜΒΑΚΑΣ ΜΙΧΑΛΗΣ)**
   h. **Μετατροπή σε pdf (ΒΑΜΒΑΚΑΣ ΜΙΧΑΛΗΣ)**
   i. **Πρόνοια (ΒΑΜΒΑΚΑΣ ΜΙΧΑΛΗΣ)**
   j. **Helpdesk (ΥΠΑΛΛΗΛΟΙ ΤΜ. ΗΛ. ΔΙΑΚ. ΚΑΙ ΔΙΑΦΑΝΕΙΑΣ)**
   k. **Σύστημα Υποστήριξης Τεχνικών Υπηρεσιών (ΠΡΩΗΝ ΥΠΑΛΛΗΛΟΣ ΤΕΧΝ. ΥΠΗΡΕΣΙΑΣ)**
   l. **Πληροφοριακό σύστημα καταγραφής εργασιών Η/Υ - e-service (ΚΑΛΑΝΤΖΗΣ ΗΛΙΑΣ)**
   m. **Πληροφοριακό σύστημα εύρεσης στοιχείων των Υπαλλήλων –e-index (ΚΑΛΑΝΤΖΗΣ ΗΛΙΑΣ)**
   n. **Μητρώο ψηφιακής υποδομής Δ. Βόλου - e-inventory (ΚΑΛΑΝΤΖΗΣ ΗΛΙΑΣ)**
   o. **Άδειες Πολεοδομίας (ΚΑΤΙΝΑΚΗ ΧΡΙΣΤΙΝΑ & ΒΑΜΒΑΚΑΣ ΜΙΧΑΛΗΣ)**

p. **Αυθαίρετα (ΚΑΤΙΝΑΚΗ ΧΡΙΣΤΙΝΑ)**

q. **Αδέσποτα Ζώα (ΚΑΤΙΝΑΚΗ ΧΡΙΣΤΙΝΑ)**

r. **Δεσποζόμενα Ζώα (ΚΑΤΙΝΑΚΗ ΧΡΙΣΤΙΝΑ)**

s. **Άδειες Υπαλλήλων (ΚΑΤΙΝΑΚΗ ΧΡΙΣΤΙΝΑ)**

t. **Διαχείριση Γραμματείας Γενικού Διευθυντή (ΚΑΤΙΝΑΚΗ ΧΡΙΣΤΙΝΑ)**

u. **Πρωτόκολλο Παράδοσης –Παραλαβής (ΚΑΤΙΝΑΚΗ ΧΡΙΣΤΙΝΑ)**

v. **Υπεύθυνη Δήλωση (ΚΑΤΙΝΑΚΗ ΧΡΙΣΤΙΝΑ)**

w. **Εγκαταλελειμμένα Οικόπεδα/Αυτοκίνητα (ΚΑΤΙΝΑΚΗ ΧΡΙΣΤΙΝΑ)**

ΕΞΩΤΕΡΙΚΕΣ ΕΦΑΡΜΟΓΕΣ (από εξωτερικούς συνεργάτες)

x. **Πληροφοριακό Σύστημα Genesis (Proset)**

y. **πληροφοριακό σύστημα Ηλεκτρονικής Διακίνησης Εγγράφων BPM (Proset)**

z. **Λογισμικό Διαχείρισης Πιστοποιημένων Διαδικτυακών Αιτημάτων Πολιτών ctservices (Proset)**

aa. **Λογισμικό Διαχείρισης Ηλεκτρονικών πληρωμών (Proset)**

bb. **ΛΟΓΙΣΜΙΚΟ ΓΙΑ ΚΑΤΑΓΡΑΦΗ ΑΙΤΗΜΑΤΩΝ ΠΟΛΙΤΩΝ ΜΕΣΩ ΚΙΝΗΤΩΝ ΤΗΛΕΦΩΝΩΝ (NOVOVILLE).**

cc. **Δομική ενημέρωση**

dd. **Verm (Λογισμικό Τοπογραφίας & Φωτογραμμετρίας) (Α&Η ΜΩΚΟΣ Ο.Ε)**

ee. **ArcGIS Desktop Basic concurrent use, ArcGIS online (ESRI)**

ff. **3DR – (3DR Engineering Software AE)**

gg. **Υπολογιστικό Η/Μ ADAPT/FCALC – (4M AE)**

hh. **ACE-ERP – (UNI-Systems)**

ii. **GG Cad – (Κων/νος Αστάρας)**

jj. **Archicad – (Top Software ΕΠΕ)**

kk. **Verm – (Α & Η Μώκος ΟΕ)**

5. Απομακρυσμένη πρόσβαση (remote access) στο εσωτερικό δίκτυο.

Οι παραπάνω προσβάσεις αφορούν τα στελέχη και το προσωπικό που εργάζεται στον Δήμο. Οι προσβάσεις αυτές καταγράφονται στο έντυπο προσβάσεων χρηστών (Έντυπο Προσβάσεων Χρηστών ΕΠ.01.01).

Επίσης, ειδική ηλεκτρονική πρόσβαση μπορεί να έχουν οι εξωτερικοί συνεργάτες με τους οποίους υπάρχει συγκεκριμένη σύμβαση έργου (π.χ. ανάπτυξη λογισμικού, παροχή συμβουλευτικών υπηρεσιών, κτλ). Στην περίπτωση αυτή ακολουθείται η ιδία διαδικασία για την έγκριση των προσβάσεων όπως αυτή που ισχύει για τα στελέχη και τους υπαλλήλους του Δήμου και συμπληρώνεται και Ατομική Καρτέλα Προσβάσεων Χρηστών. Η πρόσβαση εξωτερικών συνεργατών πρέπει να διακόπτεται άμεσα μετά την ολοκλήρωση του έργου για το οποίο δόθηκε.

1.4.1 Πρόσβαση στο λειτουργικό σύστημα και στο εσωτερικό δίκτυο

Τα δικαιώματα πρόσβασης σε λειτουργικό σύστημα windows κάθε προσωπικού σταθμού εργασίας ελέγχονται με κατάλληλο κωδικό, τον οποίο δημιουργεί ο ίδιος ο χρήστης κατά την πρώτη πρόσβαση σε περιβάλλον domain. Όταν πρόκειται για root χρήστη συστήματος (Διαχειριστή) η ανάθεση του κωδικού γίνεται από τον ΙΤ. Ο κωδικός είναι μοναδικός και γνωστός μόνο στον ίδιο το χρήστη.

Στην περίπτωση κωδικού root χρήστη (διαχειριστή), αντίγραφο του κωδικού αυτού κρατείται σε καλά ασφαλισμένο χώρο μέσα στα γραφεία της Διεύθυνσης, σύμφωνα με τα οριζόμενα στην Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων (Π.09).

1.4.2 Πρόσβαση στους file Servers

Τα δικαιώματα πρόσβασης στους file servers ελέγχονται επίσης με κατάλληλο κωδικό, ο οποίος δημιουργείται από τον ίδιο τον χρήστη κατά την πρώτη του είσοδο. Ο κωδικός είναι μοναδικός και γνωστός μόνο στον ίδιο το χρήστη με ευθύνη του. Τα δικαιώματα πρόσβασης στους εξυπηρετητές είναι διαβαθμισμένα, ορίζονται δηλαδή ανά χρήστη δικαιώματα για ανάγνωση ή/και για μεταβολή ή/και για δημιουργία ή/και για διαγραφή εγγραφών με ευθύνη του Υπεύθυνου Διαχείρισης Πληροφοριακών Συστημάτων και Δικτύων. Σε περιβάλλον workgroup τον κωδικό αναθέτει στον χρήστη ο ΙΤ.

Την ευθύνη ενημέρωσης του Γραφείου Πληροφορικής, για την δημιουργία, τροποποίηση και διαγραφή των χρηστών έχει ο προϊστάμενος κάθε διεύθυνσης που ανήκει ο χρήστης. Η ενημέρωση του Γραφείου πληροφορικής από τον προϊστάμενο της διεύθυνσης γίνεται μέσω αποστολής e-mail, με θέμα «*Δικαιώματα Χρήστη*» ή μέσω της εφαρμογής HelpDesk.

Το δικαίωμα πρόσβασης (user ID) στους file servers είναι μοναδικό για κάθε χρήστη έτσι ώστε να επιτρέπεται ο έλεγχος και να αναγνωρίζονται οι υπευθυνότητες των ενεργειών τους.

Ο Υπεύθυνος Διαχείρισης Πληροφοριακών Συστημάτων και Δικτύων πρέπει να τηρεί ενημερωμένο κατάλογο (ΕΠ.01.03) με τα ονόματα των χρηστών που έχουν πρόσβαση στους servers καταγράφοντας τα δικαιώματα που αυτοί έχουν (ανάγνωση ή/και μεταβολή ή/και δημιουργία ή/και διαγραφή εγγραφών).

1.4.3 Πρόσβαση σε ηλεκτρονικό ταχυδρομείο (email)

Τα δικαιώματα πρόσβασης σε λογαριασμό ηλεκτρονικού ταχυδρομείου του Δήμου ελέγχονται με κατάλληλο κωδικό με ευθύνη του Υπεύθυνου Διαχείρισης Πληροφοριακών Συστημάτων και Δικτύων.

Ειδικότερα ρυθμίζεται η διάρκεια διατήρησης λογαριασμού χρήστη που αποχώρησε από τον Δήμο ως εξής:

- Ο λογαριασμός διατηρείται ενεργός για περίοδο 6 μηνών μετά την αποχώρηση του υπαλλήλου.
- Ο χρήστης του λογαριασμού έχει την υποχρέωση να διαγράψει τυχόν προσωπικά μηνύματα που μπορεί να υπάρχουν στο λογαριασμό του.
- Ο λογαριασμός ανακατευθύνεται αυτόματα σε άλλον λογαριασμό ώστε να μπορεί να παρακολουθείται, για την περίοδο των 6 μηνών που θα μείνει ενεργός.
- Μετά το πέρας του παραπάνω διαστήματος όλα τα περιεχόμενα του διαγράφονται και ο λογαριασμός καταργείται από το σύστημα.

1.4.4 Πρόσβαση στο διαδίκτυο

Τα δικαιώματα πρόσβασης στο διαδίκτυο ελέγχονται από τον Υπεύθυνο Διαχείρισης Πληροφοριακών Συστημάτων και Δικτύων και δεν απαιτείται η χρήση κωδικού. Περαιτέρω έλεγχος της πρόσβασης σε διάφορους ιστότοπους μπορεί να εκτελείται μέσω ειδικής εφαρμογής φιλτραρίσματος περιεχομένου (Content Filtering).

1.4.5 Απομακρυσμένη πρόσβαση στο εσωτερικό δίκτυο (VPN)

Δικαιώματα απομακρυσμένης πρόσβασης στο εσωτερικό δίκτυο του Δήμου έχουν μόνο αυστηρά περιορισμένος αριθμός χρηστών και η αδειοδότηση απαιτεί έγκριση από την Διεύθυνση Πληροφορικής του Δήμου. Η απομακρυσμένη πρόσβαση γίνεται με τη χρήση κατάλληλου κωδικού, ο οποίος δίνεται στον κάθε χρήστη από την Διοίκηση ή τον IT. Ο κωδικός είναι μοναδικός και γνωστός μόνο στον ίδιο το χρήστη με ευθύνη του.

Η απομακρυσμένη πρόσβαση διακόπτεται αυτόματα εάν ο χρήστης σταματήσει κάθε ενέργεια για πάνω από 15’ λεπτά (Session time-out).

Η απομακρυσμένη πρόσβαση περιγράφεται αναλυτικότερα στην «Πολιτική Απομακρυσμένης Πρόσβασης – vpn – Π.02), όπως περιγράφεται στο παράρτημα Α2 του παρόντος εγγράφου».

1.4.6 Πρόσβαση σε Εφαρμογές (ERP, κλπ.)

Στον Δήμο λειτουργούν διάφορα πληροφοριακά συστήματα και εφαρμογές που ελέγχονται από την αρμόδια για την υλοποίηση Διεύθυνση. Οι χρήστες των συστημάτων αυτών έχουν κωδικό πρόσβασης ο οποίος είναι μοναδικός και προσωπικός. Αρμόδιος για τη διαχείριση των κωδικών πρόσβασης, είναι αυτός που ορίζεται από την κάθε Διεύθυνση ως διαχειριστής του συστήματος, ο οποίος θα πρέπει να διατηρεί μητρώο των χρηστών που έχουν πρόσβαση στο σύστημα καταγράφοντας και τα δικαιώματα που έχουν (ανάγνωση ή/και μεταβολή ή/και δημιουργία ή/και διαγραφή πληροφοριών), στο έντυπο ΕΠ.01.02 Έντυπο Προσβάσεων Εφαρμογής.

1.5 Διαχείριση των κωδικών

Όλοι οι κωδικοί που χρησιμοποιούνται για οποιαδήποτε πρόσβαση αποτελούνται από τουλάχιστον 8 χαρακτήρες οι οποίοι πρέπει υποχρεωτικά να είναι συνδυασμός γραμμάτων, αριθμών και συμβόλων. Οι κωδικοί είναι προσωπικοί δεν πρέπει να γνωστοποιούνται ή να κοινοποιούνται σε καμία περίπτωση. Τα ηλεκτρονικά μέσα στα οποία έχει πρόσβαση ο κάθε χρήστης καταγράφονται στο Έντυπο ΕΠ.01. 01 «Έντυπο Προσβάσεων Χρηστών» με ευθύνη του Υπεύθυνου Προστασίας Δεδομένων και σε συνεργασία με τον Υπεύθυνο Διαχείρισης Πληροφοριακών Συστημάτων και Δικτύων.

Ο Υπεύθυνος Διαχείρισης Πληροφοριακών Συστημάτων και Δικτύων ενημερώνει τον χρήστη ότι ο κωδικός είναι αυστηρά προσωπικός. Για τη διασφάλιση του αυστηρά προσωπικού κωδικού ο ΙΤ φροντίζει να είναι ενεργοποιημένη η επιλογή για αλλαγή κωδικού πριν από την πρώτη είσοδο. Ο κάθε χρήστης φέρει την ευθύνη για την διαφύλαξη των προσωπικών του κωδικών ασφαλείας. Σε περίπτωση απώλειας κάποιου κωδικού ή/και σε περίπτωση υποψίας υποκλοπής κωδικού, ο χρήστης ενημερώνει άμεσα τον Υπεύθυνο Διαχείρισης Πληροφοριακών Συστημάτων και Δικτύων ή τον αρμόδιο του σχετικού πληροφοριακού συστήματος ο οποίος αρχικοποιεί τη διαδικασία επιλογής κωδικού, ώστε να μπορεί ο χρήστης να ορίσει νέο κωδικό.

Ο Υπεύθυνος Διαχείρισης Πληροφοριακών Συστημάτων και Δικτύων πρέπει να ενημερώνει τους χρήστες για τις οδηγίες που θα πρέπει να ακολουθούν έτσι ώστε να αποτρέψουν την υποκλοπή των κωδικών τους. Οι οδηγίες αυτές είναι :

- *Να μη χρησιμοποιούν εύκολα προβλέψιμους κωδικούς (π.χ. ονοματεπώνυμα, ημερομηνία γεννήσεως κ.λπ.)*
- *Να διαμορφώνουν τους κωδικούς ώστε να περιέχουν συνδυασμό από γράμματα, σύμβολα και αριθμούς.*
- *Να απομνημονεύουν τους κωδικούς και μην τους καταγράφουν σε μέρη που μπορεί να υποκλαπούν (ατζέντες, σημειωματάρια κ.λπ.)*
- *Να αλλάζουν συχνά τους κωδικούς.*

Οι ανωτέρω αρχές για την διαχείριση των κωδικών ισχύουν και στην περίπτωση των πληροφοριακών συστημάτων με ευθύνη του αρμόδιου διαχειριστή του Συστήματος.

1.6 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ

- ΕΠ.01.01 Έντυπο Προσβάσεων Χρηστών
- ΕΠ.01.02 Έντυπο Προσβάσεων Εφαρμογής
- ΕΠ.01.03 Έντυπο Δικαιωμάτων Πρόσβασης Χρήστη

1.7 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
Έντυπο Ατομική Καρτέλα Προσβάσεων ΕΠ.01.01	Έντυπη / Ηλεκτρονική	Επ' αόριστον	Υπεύθυνος ΙΤ
Έντυπο Προσβάσεων Εφαρμογής ΕΠ.01.02	Έντυπη / Ηλεκτρονική	Επ' αόριστον	Υπεύθυνος Διαχειριστής Εφαρμογής
Έντυπο Δικαιωμάτων Πρόσβασης Χρήστη ΕΠ.01.03	Έντυπη / Ηλεκτρονική	Επ' αόριστον	Υπεύθυνος ΙΤ

2 Πολιτική Τηλεργασίας (vpn)

2.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγραφεί η μεθοδολογία διασύνδεσης από απομακρυσμένους υπολογιστές στο εσωτερικό δίκτυο και στα υπολογιστικά συστήματα του Δήμου.

2.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται για όλα τα μέσα που δύνανται να συνδέονται στο εταιρικό δίκτυο, ήτοι φορητοί υπολογιστές (laptops), κινητά τηλέφωνα, tablets κλπ.

2.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- IT

2.4 Χρήση Συσκευών

Απαγορεύεται η χρήση μη εξουσιοδοτημένων/εγκεκριμένων φορητών υπολογιστών και/ή άλλων συσκευών. Η σύνδεση μπορεί να εκτελείται μόνο από εγκεκριμένες, από το τμήμα Πληροφορικής, συσκευές. Μετά την έγκριση χρήσης οποιασδήποτε συσκευής, δεν επιτρέπεται να γίνουν τροποποιήσεις και εγκαταστάσεις νέων προγραμμάτων χωρίς την προηγούμενη άδεια του IT. Οι εξουσιοδοτημένες συσκευές μπορεί να ελέγχονται ανά τακτά χρονικά διαστήματα από τον IT.

2.4.1 Ρυθμίσεις συσκευής

Για να μπορεί να συνδεθεί μια συσκευή απομακρυσμένα στο εταιρικό δίκτυο με την υλοποίηση της τεχνολογίας vpn, θα πρέπει η συσκευή να ελεγχθεί από τον IT ότι καλύπτει ορισμένα ελάχιστα κριτήρια ασφάλειας.

2.4.2 Ελάχιστα κριτήρια ασφάλειας Η/Υ

Σαν ελάχιστα κριτήρια ασφάλειας ορίζονται τα παρακάτω:

Α. Λειτουργικό σύστημα:

Windows 10, έκδοση 1809 και νεότερη
Android έκδοση 6.0 (Marshmallow) ή iOS έκδοση 10.3.3 για κινητές συσκευές

Β. Ισχυρός κωδικός log-in χρήστη, όπως προβλέπεται από την Πολιτική Απορρήτου Κωδικών Χρηστών (Παράρτημα Α1 παρόντος).

Γ. Εγκατεστημένο πρόγραμμα antivirus

Δ. Ενεργό firewall (μόνο για υπολογιστές)

2.4.3 Ρυθμίσεις ασφαλείας vpn σύνδεσης

Όπου είναι εφικτό η σύνδεση πρέπει να ασφαλίζεται με τη χρήση ιδιωτικού / δημόσιου κλειδιού.

Για την εξασφάλιση της ασφαλούς σύνδεσης θα πρέπει να ρυθμιστεί η επίτευξη της να υλοποιείται με την χρήση εγγενούς ασφαλούς πρωτοκόλλου (Παράδειγμα IPSec).

Με τη χρήση της VPN τεχνολογίας με προσωπικό εξοπλισμό, οι χρήστες θα πρέπει να κατανοήσουν ότι τα μηχανήματα που χρησιμοποιούν για την πραγματοποίηση της σύνδεσης τους, καθίστανται προέκταση του δικτύου του Δήμου. Συνέπια τούτου είναι ότι πρέπει να ακολουθούν τις πολιτικές ασφαλείας του Δήμου και ο ιδιωτικός εξοπλισμός τους υπόκειται στους ίδιους κανόνες που εφαρμόζονται για τον εξοπλισμό του Δήμου.

2.5 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ

Ουδέν

3 Πολιτική Προστασίας Hardware και Δεδομένων

3.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγράψει τα μέσα και τις μεθόδους που χρησιμοποιούνται για τη φυσική προστασία του Hardware που χρησιμοποιείται από τον Δήμο, καθώς επίσης και για την προστασία των δεδομένων που είναι αποθηκευμένα στα υπολογιστικά συστήματα του.

3.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε προσωπικούς σταθμούς εργασίας, σε laptops και servers ιδιοκτησίας του Δήμου.

3.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- IT

3.4 ΠΕΡΙΓΡΑΦΗ

3.4.1 Φυσική προστασία Hardware

Η περιγραφόμενη πολιτική φυσικής προστασίας του Hardware περιλαμβάνει μέτρα που διασφαλίζουν τη λειτουργικότητα του συστήματος στις κάτωθι περιπτώσεις:

- Διακύμανση / πτώση ηλεκτρικού ρεύματος
- Συνθήκες λειτουργίας (θερμοκρασία και υγρασία)
- Πυρκαγιά
- Βλάβη σε επιμέρους Hardware component (πχ δίσκος, μνήμη, κάρτα)
- Απώλεια δεδομένων από λογική διαγραφή τους (εσκεμμένη ή από αμέλεια)

3.4.2 Datacenters

Τα συστήματα που είναι εγκατεστημένα σε Datacenters εξωτερικών συνεργατών του Δήμου, θα πρέπει να καλύπτονται από υπογεγραμμένη από το συνεργάτη σύμβαση.

Στα πλαίσια των συμβάσεων, οι εξωτερικοί συνεργάτες θα πρέπει να αναλαμβάνουν:

- Την παροχή αδιάλειπτου παροχής ηλεκτρικής τάσης με χρήση UPS και γεννήτριας επαρκούς φορτίου.
- Τη διατήρηση ιδανικών συνθηκών θερμοκρασίας και υγρασίας.
- Την παροχή επαρκούς πυροπροστασίας.
- Την ελεγχόμενη πρόσβαση

- Την ενημέρωση για τη φυσική θέση των εξυπηρετητών

Ο Δήμος διατηρεί ενημερωμένο αρχείο με λίστα όλων των εξωτερικών συνεργατών του το οποίο θα πρέπει να περιλαμβάνει κατ' ελάχιστο την επωνυμία του συνεργάτη, πρόσωπο και πληροφορίες επικοινωνίας.

ΣΗΜΕΙΩΣΗ: Όλες οι παραπάνω απαιτήσεις θα πρέπει να αποτυπώνονται και στη σύμβαση με τον συνεργάτη

3.4.3 Computer Room

Για τη φυσική προστασία του Hardware από απότομες διακυμάνσεις του ηλεκτρικού ρεύματος, χρησιμοποιούνται UPS τα οποία καλύπτουν όλες τις κρίσιμες συσκευές δικτύου και τους εξυπηρετητές.

Τα UPS μπορούν να καλύψουν τις ανάγκες των προαναφερθέντων στοιχείων για 20 λεπτά.

Μέσα στο διάστημα αυτό και εάν δεν αποκατασταθεί η παροχή ηλεκτρικού ρεύματος, είτε μέσω του παρόχου είτε μέσω γεννητριών εφεδρικής παροχής, ο IT θα πρέπει να βγάλει εκτός λειτουργίας τα υπολογιστικά συστήματα για την αποφυγή απώλειας δεδομένων λόγω αστοχίας υλικού.

Ενεργείται ετήσιος έλεγχος των συσκευών ελέγχου πρόσβασης, προστασίας περιβάλλοντος και των συστημάτων πρόληψης και κατάσβεσης πυρκαγιών, από τον Υπεύθυνο Ασφάλειας Κτηρίου, που εξασφαλίζουν την κανονική λειτουργία του computer room και των συστημάτων του.

Τέλος, πραγματοποιείται τακτική συντήρηση των εξυπηρετητών και των συσκευών δικτύου σύμφωνα με τις οδηγίες του κατασκευαστή. Στα πλαίσια της τακτικής συντήρησης θα εκτελείται και καθαρισμός με πεπιεσμένο αέρα.

3.4.4 Διόρθωση/επισκευή βλαβών

Στην περίπτωση που παρουσιαστεί βλάβη σε εξάρτημα εξοπλισμού για το οποίο υπάρχει εφεδρικό, η αντικατάσταση του προβληματικού εξαρτήματος γίνεται είτε εν λειτουργία (Hot Swap, αν αυτό επιτρέπεται από το σύστημα) είτε αφού το σύστημα τεθεί εκτός λειτουργίας σε προκαθορισμένο χρονικό διάστημα.

Σε κάθε περίπτωση, η αντικατάσταση γίνεται είτε από προσωπικό της Διεύθυνσης Πληροφορικής του Δήμου, είτε από προσωπικό του κατασκευαστή, οπωσδήποτε δε με ανταλλακτικό της κατασκευάστριας εταιρείας.

Στην περίπτωση που ένα σύστημα τεθεί εκτός λειτουργίας χωρίς να υπάρχει δυνατότητα αποτροπής της βλάβης, με μέριμνα του IT εξετάζεται κατά πόσον αυτό μπορεί να επισκευαστεί με ίδια μέσα. Εφόσον αυτό είναι δυνατό, η βλάβη αποκαθίσταται στο συντομότερο χρονικό διάστημα. Εφόσον αυτό δεν είναι δυνατό, καλείται η κατασκευάστρια εταιρεία να προβεί στην επισκευή του. Ο χρόνος απόκρισης της κατασκευάστριας εταιρείας, για συσκευές εντός του χρόνου εγγύησης, δεν μπορεί να είναι μεγαλύτερος της μιας εργάσιμης ημέρας (next business day). Ο παραπάνω χρονικός περιορισμός επέμβασης του κατασκευαστή, πρέπει να αποτυπώνεται και στα συμβόλαια προμήθειας και/ή συντήρησης του εξοπλισμού.

Όλα τα συστήματα που είναι εγκατεστημένα σε Datacenters θα πρέπει να καλύπτονται από τη Σύμβαση Παροχής Υπηρεσιών με τον εξωτερικό συνεργάτη.

3.5 Προστασία δεδομένων

Για την προστασία των δεδομένων που βρίσκονται αποθηκευμένα στα υπολογιστικά συστήματα του Δήμου (servers και προσωπικούς σταθμούς εργασίας) χρησιμοποιούνται τα ακόλουθα μέτρα:

3.5.1 Δεδομένα σε Servers

Τα μέτρα προστασίας των δεδομένων των εξυπηρετητών είναι τα ακόλουθα:

Κρυπτογράφηση των βάσεων δεδομένων των εξυπηρετητών (όπου κρίνεται σκόπιμο, βάσει διενέργειας εκτίμησης επικινδυνότητας και είναι εφικτό).

Εγκατάσταση Firewall.

Έλεγχος πρόσβασης όπως περιγράφεται στο Παράρτημα Α1, Πολιτική Προσβάσεων και Απορρήτου Κωδικών.

Τήρηση αντιγράφων ασφαλείας όπως περιγράφεται στο Παράρτημα Α8, Πολιτική Αντιγράφων Ασφαλείας.

Εγκατάσταση και λειτουργία antivirus & antispam: Ο IT είναι αρμόδιος για την εγκατάσταση λογισμικού antivirus και antispam στους servers. Η ενημέρωση των εφαρμογών antivirus και

antispam θα γίνεται αυτόματα τουλάχιστον σε ημερήσια βάση, ενώ θα πρέπει να εκτελείται και περιοδικός έλεγχος της ενημέρωσης του antivirus.

3.6 Προστασία & Αποτροπή Ιών

1. Όλοι οι σταθμοί εργασίας (Workstations και laptops) έχουν εγκατεστημένο το *Kaspersky Antivirus*.
2. Με κάθε εγκατάσταση νέου σταθμού εργασίας γίνεται εγκατάσταση του *Kaspersky X Antivirus* και λαμβάνονται τα τελευταία Definition Updates.
3. Μέσω Remote Administration είναι ρυθμισμένο να γίνεται Quick Scan κάθε 7 ημέρες στους σταθμούς εργασίας και κάθε 24 ώρες στους διακομιστές.
4. Ακόμα, όσες θύρες πρόσβασης σε δίκτυο δεν χρησιμοποιούνται από κάποιον υπολογιστή είναι απενεργοποιημένες στους διαμεταγωγείς (Switch) έτσι ώστε να αποφευχθεί η οποιαδήποτε πιθανότητα να συνδεθεί κάποιος μολυσμένος υπολογιστής χωρίς να έχει γίνει έλεγχος.

3.6.1 Εγκατάσταση και λειτουργία Firewall

Η λειτουργία του firewall εξασφαλίζεται από την υπηρεσία «ΣΥΖΕΥΞΙΣ». Εάν απαιτείται η χρήση ειδικής πόρτας από κάποια εφαρμογή αποστέλλεται αίτημα με e-mail, προς την υπηρεσία «ΣΥΖΕΥΞΙΣ», ώστε να ενεργοποιήσει τη σχετική ρύθμιση. Παράλληλα ενημερώνεται και το αρχείο κανόνων firewall, που διατηρείται από το Γραφείο Πληροφορικής του Δήμου.

Σε επίπεδο συσκευών χρησιμοποιείται το Cisco Umbrella (Cloud Enterprise Network Security)

3.7 Σε Desktop PC’s & Laptops

3.7.1 Firewall

Στα Desktops και Laptops έχει ενεργοποιηθεί το firewall του λειτουργικού συστήματος (Microsoft firewall).

3.7.2 Εγκατάσταση και λειτουργία antivirus & antispam

Ο ΙΤ είναι αρμόδιος για την εγκατάσταση λογισμικού antivirus και antispam στους φορητούς και τους προσωπικούς σταθμούς εργασίας του προσωπικού. Η ενημέρωση των virus definitions θα

γίνεται αυτόματα σε ημερήσια βάση, ενώ ο IT είναι αρμόδιος για τον περιοδικό έλεγχο της ενημέρωσης του antivirus.

Στους σταθερούς σταθμούς εργασίας (PC), έχει εγκατασταθεί το *Kaspersky Antivirus*, το οποίο ενημερώνεται αυτόματα από το site του προμηθευτή.

3.7.3 Καθορισμός δικαιωμάτων πρόσβασης

Σε κάθε σταθερό και φορητό ηλεκτρονικό υπολογιστή καθορίζονται δικαιώματα κωδικοί πρόσβασης στον υπολογιστή, πρόσβασης στο δίκτυο και πρόσβασης στις εφαρμογές. Τα σχετικά με τα δικαιώματα πρόσβασης περιγράφονται στο Παράρτημα Α1. (Πολιτική Προσβάσεων και Απορρήτου Κωδικών Χρηστών – Π.01).

3.8 Κρυπτογράφηση

Τα δεδομένα των laptops και κατά περίπτωση των desktops, κρυπτογραφούνται με τη χρήση της εφαρμογής bitlocker του λειτουργικού συστήματος windows. Στην περίπτωση χρήσης άλλων λειτουργικών που δεν διαθέτουν εφαρμογή κρυπτογράφησης θα πρέπει να χρησιμοποιηθεί ειδικό λογισμικό.

Στην ιστοσελίδα του Δήμου θα πρέπει να γίνεται χρήση του πρωτοκόλλου Secure Socket Layer (SSL) και ιδιαίτερα σε σελίδες που απαιτούν τη χρήση συνθηματικών για την πιστοποίηση του εκάστοτε χρήστη που επιθυμεί πρόσβαση. Επίσης απαιτείται η χρήση SSL σε σελίδες που διαθέτουν πεδία όπου ο χρήστης πρέπει να εισάγει δεδομένα, όπως για παράδειγμα σε μία φόρμα επικοινωνίας.

Περισσότερες λεπτομέρειες σχετικά με τις μορφές κρυπτογράφησης για τον Δήμο, παραθέτονται στην Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων (Π.08).

3.9 Συνημμένα Έντυπα

ΟΥΔΕΝ

4 Πολιτική Χρήσης Αφαιρούμενων Μέσων

4.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγραφεί η μεθοδολογία διαχείρισης των φορητών μέσων που επεξεργάζονται, αποθηκεύουν ή δύνανται να έχουν πρόσβαση σε δεδομένα που είναι αποθηκευμένα στα υπολογιστικά συστήματα του Δήμου.

4.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε όλα τα φορητά μέσα που δύνανται να επεξεργάζονται / διαχειρίζονται / αποθηκεύουν πληροφοριακά δεδομένα, ήτοι φορητοί υπολογιστές (laptops), κινητά τηλέφωνα και αφαιρούμενοι δίσκοι και μέσα (εξωτερικοί δίσκοι, CDs, DVDs, USB flash disks κλπ).

4.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- IT
- Υπάλληλοι

4.4 ΠΕΡΙΓΡΑΦΗ

4.4.1 Χρήση Laptops

Απαγορεύεται η χρήση μη εξουσιοδοτημένων / εγκεκριμένων φορητών υπολογιστών. Η χρήση των εφαρμογών γίνεται μόνο από τα εξουσιοδοτημένα Desktops ή Laptops ιδιοκτησίας του Δήμου ή από φορητές συσκευές που υπόκεινται σε καθεστώς BYOD.

4.4.2 Χρήση Κινητών Τηλεφώνων

Κατά τη χρήση των κινητών τηλεφώνων από το προσωπικό τηρούνται οι ακόλουθοι κανόνες ασφαλείας:

- Επιτρέπεται γενικά η χρήση κινητών τηλεφώνων για φωνητικές κλήσεις και γραπτά μηνύματα από το προσωπικό με τέτοιον τρόπο που να διαφυλάσσει την εμπιστευτικότητα των πληροφοριακών δεδομένων.
- Δεν επιτρέπονται οι βιντεοκλήσεις και η εν γένει η χρήση της κάμερας και της λειτουργίας ηχογράφησης σε όσα κινητά τηλέφωνα διαθέτουν τα ανωτέρω χαρακτηριστικά.

4.4.3 Χρήση Αφαιρούμενων Δίσκων και μέσων (εξωτερικοί δίσκοι, CDs, DVDs, USB flash disks κλπ)

Επιτρέπεται στο προσωπικό η εγγραφή μόνο πληροφοριακών δεδομένων που δεν έχουν χαρακτηρισθεί σαν εμπιστευτικά ή απόρρητα, σε εξωτερικούς δίσκους ή αποθηκευτικά μέσα οποιασδήποτε μορφής και η μεταφορά του φορητού μέσου αποθήκευσης εκτός των χώρων του Δήμου.

Δεν επιτρέπεται στο προσωπικό η εγγραφή πληροφοριακών δεδομένων που έχουν χαρακτηρισθεί σαν **εμπιστευτικά** (απλά προσωπικά δεδομένα) σε εξωτερικούς δίσκους ή αποθηκευτικά μέσα οποιασδήποτε μορφής και η μεταφορά του φορητού μέσου αποθήκευσης εκτός των χώρων του Δήμου χωρίς εξουσιοδότηση / άδεια από τον Διευθυντή της Διεύθυνσης.

Η μόνη μεταφορά πληροφοριακών δεδομένων που επιτρέπεται είναι, εάν απαιτείται αποθήκευση του Backup σε εξωτερικό χώρο.

Έγγραφα που έχουν χαρακτηρισθεί ως **απόρρητα (ευαίσθητα προσωπικά δεδομένα) απαγορεύεται** να μεταφερθούν με φορητό αποθηκευτικό μέσο εάν αυτό δεν είναι κρυπτογραφημένο.

5 Πολιτική Ασφαλείας Δικτύου και Συστημάτων

5.1 ΣΚΟΠΟΣ

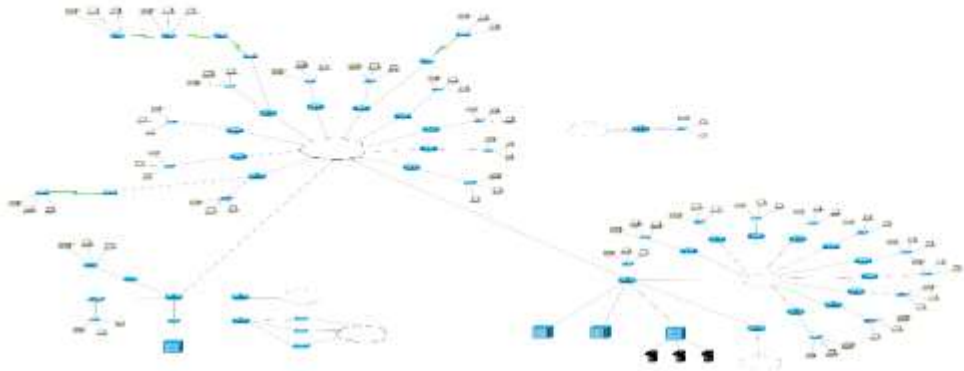
Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι η περιγραφή των τεχνικών που ακολουθούνται για την ασφάλεια του Δικτύου και των Συστημάτων του Δήμου.

5.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε όλα σε όλα τα συστήματα και τα δίκτυα που χρησιμοποιούνται κατά τις λειτουργίες του Δήμου.

Η τοπολογία του δικτύου και των συστημάτων απεικονίζεται παρακάτω:

ΑΠΛΟΥΣΤΕΥΜΕΝΟ ΔΙΑΓΡΑΜΜΑ ΔΙΚΤΥΟΥ



5.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Υπεύθυνος Προστασίας Δεδομένων
- IT

5.4 ΠΕΡΙΓΡΑΦΗ

5.4.1 Ασφάλεια Περιμέτρου

Σκοπός της πολιτικής ασφάλειας περιμέτρου είναι να διατηρήσει ένα ικανοποιητικό επίπεδο ασφάλειας, ιδιαίτερα όσον αφορά την πρόσβαση από και προς το Internet. Η πολιτική ασφάλειας περιμέτρου ορίζει τους μηχανισμούς (σε υλικό και λογισμικό) που χρησιμοποιούνται για το σκοπό αυτό καθώς και τους τρόπους διαμόρφωσης και ανανέωσης αυτών. Τέτοιοι μηχανισμοί είναι τα συστήματα Firewall και η κατάτμηση του δικτύου σε χωριστά λογικά δίκτυα, στα οποία επιτρέπεται η διακίνηση ορισμένου είδους πληροφορίας και μόνο.

Η διαθεσιμότητα και η προστασία του πληροφοριακού συστήματος του Δήμου εξασφαλίζεται σε δύο επίπεδα:

Α. Σε επίπεδο λογισμικού εφαρμογών με τη χρήση του ενσωματωμένου firewall των Windows

Β. Σε επίπεδο μεταφοράς με τη χρήση του firewall της υπηρεσίας «ΣΥΖΕΥΞΙΣ».

Γ. Σε επίπεδο Εξυπηρετητή με τη χρήση του Kaspersky Firewall.

Δ. Σε επίπεδο Συσκευών με το Cisco Umbrella (Cloud Enterprise Network Security)

Πρόσβαση στο διαδίκτυο έχουν όλα τα συστήματα του Δήμου, με κατεύθυνση της κίνησης από το εσωτερικό δίκτυο προς τα έξω. Η πρόσβαση γίνεται με χρήση του πρωτοκόλλου NAT (Network Address Translation) ώστε όλα τα πακέτα δεδομένων που διέρχονται από το firewall να εξέρχονται με την public IP address αυτού και να μη γίνεται γνωστή η διεύθυνση του server.

Η διαμόρφωση και ανανέωση των firewalls ακολουθεί τις διεθνώς αποδεκτές πρακτικές, όπως οι παρακάτω:

1. Η διαμόρφωση των firewall δεν επιτρέπει την εισερχόμενη κίνηση σε κανένα πακέτο και σύνδεση εκτός εάν ο τύπος της κίνησης και της σύνδεσης έχει ρητώς επιτραπεί.
2. Οι κανόνες του firewall καθορίζονται από την πολιτική ασφάλειας δικτύου.

3. Επιτρέπεται η είσοδος από το διαδίκτυο προς το εσωτερικό δίκτυο μόνο εκείνων των δικτυακών συνόδων, οι οποίες έχουν ισχυρή ταυτοποίηση και κρυπτογράφηση και αφορούν την διαχείριση των υπηρεσιών του Δήμου.
4. Το Firewall του Data Center ελέγχεται και παρακολουθείται συνεχώς.
5. Ο Υπεύθυνος Ασφάλειας Πληροφοριών τηρεί γραπτή τεκμηρίωση της διαμόρφωσης και λειτουργίας των firewalls, διάγραμμα του δικτύου και των διευθύνσεων IP, καθώς και των υπηρεσιών και των τύπων κίνησης που εξουσιοδοτούνται να διατρέξουν τα firewalls. Επίσης στοιχεία που αφορούν τις υπηρεσίες και τους σταθμούς εργασίας, οι οποίοι εξουσιοδοτούνται να επικοινωνούν για λόγους παραμετροποίησης με την συσκευή Firewall.

5.4.2 Πολιτική ασφάλειας συστημάτων

Όλες οι προμήθειες συστημάτων βασίζονται σε προδιαγραφές, οι οποίες λαμβάνουν υπόψη και τα ζητήματα ασφάλειας. Οι προδιαγραφές ασφάλειας ελέγχονται από τον Υπεύθυνο Ασφάλειας, καθώς και από τη διεύθυνση που θα αναλάβει τη διαχείριση των συστημάτων έπειτα από την εγκατάστασή τους.

Όλα τα συστήματα ελέγχονται και τίθενται σε δοκιμαστική λειτουργία πριν τεθούν σε παραγωγική λειτουργία. Όλα τα συστήματα, ανεξαρτήτως μεγέθους και πολυπλοκότητας, που αναπτύσσονται από στελέχη του Δήμου ενσωματώνουν επαρκείς μηχανισμούς ασφάλειας. Ιδιαίτερη προσοχή αποδίδεται στην αυθεντικοποίηση (authentication) και τον έλεγχο πρόσβασης των χρηστών. Για τις εφαρμογές που αναπτύσσονται από τον Δήμο απαραίτητη είναι και η ύπαρξη τεκμηρίωσης της εφαρμογής (Technical Manual).

Όλους τους servers που χρησιμοποιεί ο Δήμος πρέπει να τους χειρίζεται μια, ικανή ομάδα ή άτομο (εσωτερική ή εξωτερική) η οποία θα είναι υπεύθυνη για τη διαχείριση τους. Κάθε ομάδα ή άτομο θα πρέπει να δημιουργήσει οδηγίες ρυθμίσεων, τις οποίες θα πρέπει να συντηρεί και να αναβαθμίζει. Αυτές οι οδηγίες θα πρέπει να βασίζονται στις επιχειρησιακές ανάγκες του Δήμου και να εγκριθούν από τον Δήμο που έχει σχεδιάσει τις πολιτικές ασφαλείας.

Τα ελάχιστα στοιχεία τα οποία πρέπει να διατηρούνται είναι:

- Η τοποθεσία του server
- Ο τύπος του υλικού
- Η έκδοση του λειτουργικού συστήματος
- Οι κύριες λειτουργίες που εξυπηρετεί

- Οι εφαρμογές που τρέχει
- Στοιχεία επαφής με τον υπεύθυνο για τον server
- Κρισιμότητα λόγω αποθήκευσης / επεξεργασίας δεδομένων

Οι παραπάνω πληροφορίες θα πρέπει να ενημερώνονται σε κάθε αλλαγή τους. Οι αλλαγές των ρυθμίσεων των servers θα πρέπει να γίνονται με βάση τις ανάλογες διαδικασίες που έχουν οριστεί. Όλα τα παραπάνω στοιχεία πρέπει να αποτυπώνονται στο έντυπο ΕΠ.05.1 – Μητρώο Συσκευών.

5.4.3 Παρακολούθηση (Monitoring) και Έλεγχος

Όλα τα γεγονότα που σχετίζονται με την ασφάλεια ευαίσθητων συστημάτων πρέπει να καταγράφονται και να ελέγχονται σύμφωνα με τα παρακάτω.

- Όλα τα security logs των συστημάτων και των εφαρμογών, παραμένουν διαθέσιμα στο δίκτυο για τουλάχιστον ένα έτος. (ΔΙΑΤΗΡΟΥΝΤΑΙ ΓΙΑ 1 ΕΤΟΣ)
    - Για την τεκμηρίωση των αρχείων καταγραφών θα διατηρείται το έντυπο ΕΠ.05.02 – Λίστα Αρχείων Καταγραφών
- Ημερήσια (προσθετικά) backups θα πρέπει να λαμβάνονται για τουλάχιστον ένα μήνα.
- Τα backups του κάθε μήνα θα πρέπει να διατηρούνται για ένα έτος. .(ΔΙΑΤΗΡΕΙΤΑΙ ΓΙΑ 1 ΕΤΟΣ)
- Γεγονότα που σχετίζονται με την ασφάλεια των συστημάτων θα πρέπει να αναφέρονται στους υπεύθυνους κι έπειτα να εξετάζονται. Στην συνέχεια θα πρέπει να οριστούν διορθωτικά μέτρα.

Μερικά χαρακτηριστικά γεγονότα που σχετίζονται με την ασφάλεια είναι:

- ❖ Port Scanning
- ❖ Στοιχεία μη εγκεκριμένης πρόσβασης ιδιαιτέρα σε διαχειριστικούς λογαριασμούς, αλλά και λογαριασμούς χρηστών
- ❖ Ασυνήθιστα περιστατικά που δεν προέρχονται από τη συνήθη χρήση κάποιας συγκεκριμένης εφαρμογής του συστήματος
- ❖ Υπέρμετρη χρήση των πόρων του δικτύου

Σε τακτά χρονικά διαστήματα θα πρέπει να διενεργούνται έλεγχοι στα μηχανήματα του Δήμου. Τα αποτελέσματα θα πρέπει να μελετώνται και στη συνέχεια να παρέχονται λύσεις. Κάθε δυνατή

προσπάθεια πρέπει να καταβάλλεται ώστε κατά την διάρκεια των ελέγχων να μην εμποδίζεται η ομαλή λειτουργία του Δήμου.

5.4.4 Χρήση VPN – Remote Access

Είναι ευθύνη των υπαλλήλων με τα δικαιώματα χρήσης του VPN να εξασφαλίσουν ότι οι μη εξουσιοδοτημένοι χρήστες δεν θα αποκτήσουν πρόσβαση στο δίκτυο του Δήμου

- Η χρήση του VPN πρέπει να ελέγχεται με τη χρήση διαφορετικού κωδικού πρόσβασης για κάθε χρήστη ή με το σύστημα δημοσίου/ιδιωτικού κλειδιού με μία ισχυρή passphrase.
- Όταν υπάρχει ενεργή σύνδεση στο δίκτυο του Δήμου, θα εξαναγκάσει όλη την κίνηση προς και από τον υπολογιστή μέσω της σύνδεσης VPN. Έτσι όλη η υπόλοιπη κίνηση θα σταματήσει.
- Όλοι οι υπολογιστές οι οποίοι συνδέονται στο εσωτερικό δίκτυο του Δήμου μέσω VPN, θα πρέπει να χρησιμοποιούν ενημερωμένο antivirus λογισμικό.
- Οι χρήστες VPN θα αποσυνδέονται αυτόματα από το δίκτυο του Δήμου μετά από δεκαπέντε λεπτά μη ενεργούς δράσης. Ο χρήστης θα πρέπει να ξανασυνδεθεί στο δίκτυο.
- Οι χρήστες οι οποίοι χρησιμοποιούν εξοπλισμό που δεν ανήκει στον Δήμο, θα πρέπει να κάνουν τις κατάλληλες ρυθμίσεις ώστε να συμμορφωθούν τα μηχανήματα που πρόκειται να χρησιμοποιήσουν με το VPN δίκτυο του Δήμου και την Πολιτική Ασφαλείας του δικτύου του.
- Με τη χρήση της VPN τεχνολογίας με προσωπικό εξοπλισμό, οι χρήστες θα πρέπει να κατανοήσουν ότι τα μηχανήματα τους είναι η προέκταση του δικτύου, και υπόκεινται στους ίδιους κανόνες και κανονισμούς που εφαρμόζονται και στον εξοπλισμό του Δήμου.

5.4.5 Πολιτική ασφάλειας fileserver

Η πρόσβαση επιτυγχάνεται μέσω του Active Directory.

Η πρόσβαση γίνεται μέσω κωδικού πρόσβασης, και ο κάθε χρήστης έχει συγκεκριμένα δικαιώματα πρόσβασης.

5.4.6 Ενημέρωση λογισμικού

Ο Υπεύθυνος Διαχειριστής Συστήματος αξιολογεί κάθε νέα έκδοση του λογισμικού των συστημάτων που αφορούν τις υπηρεσίες και αποφασίζει εάν είναι αναγκαία η ανανέωσή του. Όλες οι προτεινόμενες από τον κατασκευαστή τροποποιήσεις (patches), αναγκαίες για την ασφάλεια του συστήματος υλοποιούνται το συντομότερο δυνατό.

5.5 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ

Σε περίπτωση διαπίστωσης παραβίασης κάποιας από τις υποχρεώσεις των χρηστών, ο Δήμος έχει δικαίωμα, όταν κρίνεται απαραίτητο, ακόμη και χωρίς προειδοποίηση λόγω διαχειριστικών αναγκών, να αναστείλει τη σύνδεση του χρήστη στο δίκτυο δεδομένων ή τη πρόσβαση του σε συγκεκριμένες υπηρεσίες και να προβεί σε ενέργειες για την άρση του απορρήτου.

5.6 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ

- Ουδέν

6. ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
Τοπολογία Δικτύου	Ηλεκτρονική	Επ’ αόριστο	IT
Λίστα Κανόνων Firewall	Ηλεκτρονική	Επ’ αόριστο	IT

6 Πολιτική Αντιγράφων Ασφαλείας

6.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας πολιτικής είναι η περιγραφή των απαραίτητων ενεργειών για τη λήψη, τον έλεγχο και την ανάκτηση αντιγράφων ασφαλείας κάθε τύπου δεδομένων που χρήζουν δημιουργίας αντιγράφων ασφαλείας του Δήμου.

6.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα πολιτική εφαρμόζεται μόνο στα κεντρικά συστήματα του Δήμου (κεντρικοί εξυπηρετητές και δικτυακές συσκευές). Δεν εφαρμόζεται πολιτική αντιγράφων ασφαλείας για τους σταθμούς εργασίας των υπαλλήλων.

6.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- IT

6.4 Δημιουργία Αντιγράφων Ασφαλείας Συστημάτων

Με σκοπό την εξασφάλιση των δεδομένων σε μορφή backup υπάρχουν δύο σημεία που διατηρούνται αντίγραφα ασφαλείας, εντός και εκτός των εγκαταστάσεων του Δήμου.

Α. Στον Δήμο υπάρχουν 2 QNAP Storage, χωρητικότητας 14TB, τα οποία λειτουργούν ανεξάρτητα, και είναι συνδεδεμένο στο Storage LAN του δικτυού.

(ΕΧΟΥΜΕ 2 QNAP STORAGE ΧΩΡΗΤ. 14TB ,14TB)

Για κάθε server τρέχει ένα backup job και εκτελείται μία φορά την εβδομάδα, εναλλάξ σε διαφορετικό δίσκο με προστασία κρυπτογράφησης των δεδομένων AES256.

Με αυτό τον τρόπο δημιουργείτε ένα full image backup όλων των server του Δήμου:

- Domain Controller
- File server

- SQL servers

Β. Εκτός δομών Δήμου δεν διατηρείται αντίγραφο ασφαλείας. Το 2ο αντίγραφο ασφάλειας διατηρείται σε διαφορετικό κτίριο

6.5 Παρακολούθηση αντιγράφων ασφαλείας

Πραγματοποιείται καθημερινός έλεγχος λήψης των αντιγράφων ασφαλείας. Ο έλεγχος γίνεται αυτόματα μέσω της εφαρμογής network, από την οποία λαμβάνεται μήνυμα επιτυχούς ή ανεπιτυχούς δημιουργίας του αντιγράφου ασφαλείας. Σε περίπτωση που το παραγόμενο αντίγραφο δημιουργείται χειροκίνητα (μέσω scripting), ο διαχειριστής του συστήματος είναι υπεύθυνος για τον έλεγχο της εκτέλεσης του αντιγράφου του συστήματός του.

Εάν για κάποια υπηρεσία δεν έχει ολοκληρωθεί επιτυχώς η δημιουργία αντιγράφων ασφαλείας, η διαδικασία που ακολουθείται είναι η παρακάτω:

- Πραγματοποιείται έλεγχος του σφάλματος που εμφανίζεται.
- Πραγματοποιείται έλεγχος στο αρχείο καταγραφής του ή των υπολογιστών που λειτουργεί η υπηρεσία.
- Γίνεται επιδιόρθωση του προβλήματος που επηρέασε την διαδικασία αντιγράφων ασφαλείας.
- Εκκινείται χειροκίνητα η εκτέλεση της λήψης αντιγράφου ασφαλείας, όταν αυτό είναι εφικτό.

6.6 Ανάκτηση αντιγράφων ασφαλείας

Στην περίπτωση που απαιτείται η ανάκτηση αντιγράφων ασφαλείας για υπηρεσίες εσωτερικής χρήσης, η διαδικασία που ακολουθείται είναι η κάτωθι:

- Σύνδεση στον Server που είναι αποθηκευμένη η υπηρεσία ή το σύστημα που χρειάζεται να ανακτηθεί.
- Ανάκτηση της υπηρεσίας ή του συστήματος σε δοκιμαστικό περιβάλλον.
- Έλεγχος ορθής λειτουργίας της υπηρεσίας ή του συστήματος.

- Ανάκτηση της υπηρεσίας ή του συστήματος στο περιβάλλον λειτουργίας.

6.7 Έλεγχος αντιγράφων ασφαλείας

Για τον έλεγχο ορθής αντιγραφής υπηρεσιών και συστημάτων πραγματοποιείται μηνιαίος έλεγχος. Η διαδικασία που ακολουθείται είναι η παρακάτω:

- Ανάκτηση τυχαίων υπηρεσιών και συστημάτων σε δοκιμαστικό περιβάλλον.
- Έλεγχος ορθής λειτουργίας υπηρεσιών και συστημάτων.
- Καταγραφή υπηρεσιών και συστημάτων που ελέγχθηκαν.

6.8 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
Αντίγραφο Ασφαλείας 1	Ηλεκτρονική	1 έτος	IT
Αντίγραφο Ασφαλείας 2	Ηλεκτρονική	6 μήνες	IT

7 Πολιτική Καθαρού Γραφείου και Καθαρής Οθόνης

7.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγραφούν οι διαδικαστικές λεπτομέρειες για την τήρηση των απαιτήσεων «καθαρού γραφείου και καθαρής οθόνης» τις οποίες έχει θέσει ο Δήμος, ώστε να επιτυγχάνεται η ελαχιστοποίηση των κινδύνων για την ασφάλεια των δεδομένων.

7.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται από όλο το προσωπικό το οποίο απασχολείται με εργασίες γραφείου και / ή χειρίζεται Η/Υ.

7.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- ΙΤ

7.4 ΠΕΡΙΓΡΑΦΗ

Οι υπάλληλοι όλων των τμημάτων, που εκτελούν εργασίες γραφείου και / ή χειρίζονται Η/Υ θα πρέπει με δική τους ευθύνη:

- ✓ Να μην αφήνουν στον χώρο εργασίας τους εμπιστευτικά και απόρρητα έγγραφα πριν αποχωρήσουν από το γραφείο τους για σχετικά μεγάλα χρονικά διαστήματα μέσα στην ημέρα. Στην περίπτωση αυτή θα πρέπει να κλειδώνεται η πόρτα του γραφείου.
- ✓ Να μην αφήνουν στον χώρο εργασίας τους εμπιστευτικά και απόρρητα έγγραφα πριν αποχωρήσουν στο τέλος της ημέρας αλλά να τα τοποθετούν μέσα σε ειδικούς αποθηκευτικούς χώρους και να τα κλειδώνουν.
- ✓ Να χρησιμοποιούν τους ειδικούς καταστροφείς εγγράφων για εμπιστευτικά και απόρρητα έγγραφα τα οποία δεν χρειάζονται πλέον.
- ✓ Να γίνεται χρήση του συνδυασμού πλήκτρου WIN+L για το άμεσο κλείδωμα του Η/Υ (σε συστήματα windows).
- ✓ Να διασφαλίζουν ότι σε περίπτωση απουσίας τους από τη θέση εργασίας τους για πάνω από 10 λεπτά, ο Η/Υ που χρησιμοποιούν κλειδώνει και η επανενεργοποίησή του απαιτεί χρήση κωδικού, ο οποίος τηρείται μυστικός.

8 Πολιτική Ασφαλείας Κρυπτογραφικών Ελέγχων

8.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να αναφέρει τους κρυπτογραφικούς αλγόριθμους που χρησιμοποιούνται στα πληροφοριακά συστήματα του Δήμου και τις θέσεις φύλαξης κλειδιών και κωδικών.

8.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται στους διακομιστές του Δήμου, στα αφαιρούμενα μέσα και στα έγγραφα που περιέχουν προσωπικά δεδομένα και βρίσκονται σε αφαιρούμενα μέσα.

8.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- IT
- Υπάλληλοι

8.4 ΠΕΡΙΓΡΑΦΗ

8.4.1. Πολιτική Χρήσης Κρυπτογραφικών Αλγόριθμων

8.4.1.1. Σε όλες τις εφαρμογές παγκόσμιου ιστού (Web based applications) οι οποίες φιλοξενούνται στους διακομιστές του Δήμου ή σε συνεργάτη, γίνεται χρήση του πρωτοκόλλου Secure Sockets Layer (SSL) και πρωτίστως κατά την πιστοποίηση του εκάστοτε χρήστη που επιθυμεί πρόσβαση σε κάποια από τις παρεχόμενες υπηρεσίες.

8.4.1.2. Όλα τα ψηφιακά αφαιρούμενα μέσα που πρόκειται να μεταφερθούν εκτός των εγκαταστάσεων του Δήμου, πρέπει να είναι κρυπτογραφημένα. Το άτομο που προετοίμασε το αφαιρούμενο μέσο, φέρει την ευθύνη κρυπτογράφησής του και το άτομο που θα εκτελέσει τη μεταφορά φέρει την ευθύνη επιβεβαίωσης της εφαρμογής κρυπτογράφησης.

8.4.2. Πολιτική Διατήρησης Κρυπτογραφικών Κλειδιών

8.4.2.1. Με σκοπό την ασφαλή φύλαξη των κρυπτογραφικών κλειδιών και κωδικών που χρησιμοποιούνται από τους διαχειριστές των συστημάτων του Δήμου ορίζονται οι δύο παρακάτω θέσεις ασφαλούς φύλαξης αυτών:

Α. Κλειδωμένο Συρτάρι Γραφείου Διεύθυνσης

Β. Χρηματοκιβώτιο χώρου . . . . .

8.4.2.2. Όλοι οι διαχειριστές που κάνουν χρήση κλειδιού ή κωδικού θα παραδίδουν στο τμήμα Ηλεκτρονικής Διακυβέρνησης το κλειδί ή κωδικό τους, μέσα σε δύο σφραγισμένους φακέλους οι οποίοι θα αποθηκεύονται στις ορισμένες θέσεις. Η μόνη ένδειξη στο εξωτερικό του φακέλου θα είναι μόνο το ονοματεπώνυμο του χρήστη.

8.4.2.3 Οι υπάλληλοι ή τα στελέχη του Δήμου που διαθέτουν ψηφιακή υπογραφή πρέπει να τηρούν τη συσκευή αυθεντικοποίησης σε ασφαλές μέρος όταν δεν βρίσκονται στον υπολογιστή τους. Η συσκευή θα πρέπει να είναι καταγεγραμμένη στο Μητρώο Συσκευών πληροφορικής.

8.5 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ

Ουδέν

8.6 ΑΡΧΕΙΑ

Ουδέν

9 Πολιτική Ορθής Χρήσης Σταθμών Εργασίας

9.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής είναι να θέσει το πλαίσιο και τους κανονισμούς βάσει των οποίων γίνεται χρήση των Σταθμών Εργασίας από τα στελέχη και τους υπαλλήλους της του Δήμου καθώς και η πρόσβαση αυτών στο Διαδίκτυο.

9.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται από όλους τους χρήστες του δικτύου πληροφορικής του Δήμου.

9.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Στελέχη και Υπάλληλοι του Δήμου.

9.4 ΠΕΡΙΓΡΑΦΗ

9.4.1 *Αποδεκτή Χρήση Σταθμών Εργασίας και Πρόσβασης στο Διαδίκτυο*

Σκοπός της παρούσας Πολιτικής είναι να θέσει το πλαίσιο και τους κανονισμούς βάσει των οποίων γίνεται χρήση των Σταθμών Εργασίας από τους υπαλλήλους της εταιρείας καθώς και η πρόσβαση αυτών στο Διαδίκτυο.

9.4.2 Πεδίο Εφαρμογής

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε όλους τους χρήστες της εταιρείας.

9.4.3 Υπεύθυνος Εφαρμογής της Πολιτικής

- IT Manager

9.4.4 *Αποδεκτή Χρήση Σταθμών Εργασίας και Πρόσβασης στο Διαδίκτυο*

1. Οι λογαριασμοί των χρηστών βρίσκονται στους *Domain Controllers* του Active Directory και οι κωδικοί πρόσβασης είναι επίσης αποθηκευμένοι σε αυτούς.
2. Όλοι οι χρήστες έχουν δικαιώματα *Domain User* στους σταθμούς εργασίας.
3. Όλοι οι χρήστες της εταιρείας, εκτός από τον IT Manager, δεν μπορούν να εκτελέσουν κάποιο άλλο εκτελέσιμο αρχείο εκτός από αυτά που είναι ήδη εγκατεστημένα στον υπολογιστή τους.
4. Όλοι οι σταθμοί εργασίας κλειδώνουν όταν είναι ανενεργός ο χρήστης για περισσότερο από 10’. Για να ξεκλειδώσουν χρειάζεται να εισαχθεί το *Username* και *Password* από τον χρήστη.
5. Κάθε σταθμός εργασίας έχει εγκατεστημένο Antivirus software για προστασία από ιούς, trojans κλπ.

9.4.5 Μη αποδεκτή χρήση συστημάτων

Η παρακάτω λίστα δεν είναι εξαντλητική αλλά παρέχει ένα πλαίσιο ενεργειών που θεωρούνται μη αποδεκτές. Δεν επιτρέπεται:

- Να χρησιμοποιείτε τα συστήματα του Δήμου για παράνομες δραστηριότητες.
- Να χρησιμοποιείτε συσκευές ή λογισμικό που δεν έχει εγκριθεί
- Να χρησιμοποιείτε συστήματα που δεν ανήκουν στον Δήμο για την εκτέλεση εργασιών του Δήμου.
- Να χρησιμοποιείτε συστήματα του Δήμου για προσωπικές εργασίες.
- Να αποκαλύπτετε οποιαδήποτε δεδομένα αφορούν τον Δήμο σε τρίτους.
- Να παραβιάζονται κανόνες των πνευματικών δικαιωμάτων κάθε ιδιώτη ή εταιρίας τα οποία προστατεύονται από copyright, εμπορικό απόρρητο, πατέντες, νόμους και κανονισμούς.
- Η μη εξουσιοδοτημένη αντιγραφή προστατευόμενου από copyright υλικού όπως φωτογραφίες, βιβλία, προγράμματα-κώδικες, λογισμικό, τεχνικές πληροφορίες.
- Να χρησιμοποιείτε το ηλεκτρονικό ταχυδρομείο για την αποστολή εμπιστευτικών πληροφοριών σε παραλήπτες εκτός του Δήμου.
- Η αποστολή οποιουδήποτε άλλου e-mail εκτός αυτών που είναι απαραίτητα για την διεκπεραίωση των καθηκόντων του εργαζόμενου.
- Η αποστολή fake-mails, η προώθηση οποιουδήποτε e-mail τύπου “chain letter” κλπ
- Να επισκέπτεστε Ιστότοπους (Web Sites) με παράνομο λογισμικό, μη πρέπον υλικό ή άλλο πειρατικό οπτικοακουστικό υλικό.
- Η αποκάλυψη των κωδικών πρόσβασης σε τρίτους ή χρήση του προσωπικού λογαριασμού από άλλους.
- Η παράκαμψη της ταυτοποίησης του χρήστη ή οποιασδήποτε διαδικασίας ασφάλειας για κάθε υπολογιστή ή λογαριασμό.
- Η εισαγωγή κακόβουλων προγραμμάτων στο δίκτυο και τους υπολογιστές του Δήμου (πχ ιοί ή άλλα βλαβερά προγράμματα – malware)
- Ενέργειες όπως το port-scanning, network monitoring απαγορεύονται αυστηρά, εκτός και αν περιλαμβάνονται στα καθήκοντα του εργαζόμενου και έχει προηγουμένως ειδοποιηθεί η ομάδα IT η άδεια της οποίας απαιτείται.

- Οποιαδήποτε κακόβουλη ενέργεια προς υπολογιστές άλλους από αυτούς του χρήστη, όπως άρνησης παροχής υπηρεσιών (DoS attacks), terminating user sessions.
- Η διαφήμιση απατηλών προσφορών μέσω του Internet, χρησιμοποιώντας την υποδομή του Δήμου
- Η άσκηση εμπορικών δραστηριοτήτων μέσω του δικτύου δεδομένων του Δήμου όπως η πώληση αγαθών ή υπηρεσιών, η υπεκμίσθωση χωρητικότητας.

9.4.6 Πρόσβαση Διαδυκτιακών Τόπων

Σύμφωνα με την παρούσα Πολιτική Ασφάλειας, στους χρήστες του Δήμου επιτρέπεται η πρόσβαση στο διαδίκτυο χωρίς περιορισμούς. Ενδέχεται, για σκοπούς ασφάλειας, να εκτελείται φιλτράρισμα περιεχομένου μέσω του firewall του οργανισμού.

9.5 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ

Ουδέν

9.6 ΑΡΧΕΙΑ

Ουδέν

10 Πολιτική Ασφαλούς Μεταφοράς Πληροφοριών

10.1 Γενικά

Υπάρχουν πολλές περιπτώσεις κατά τις οποίες μεταφέρονται πληροφορίες εσωτερικά μεταξύ διευθύνσεων / τμημάτων ενός Δήμου και εξωτερικά, σε εταιρείες και σε ιδιώτες. Αυτό γίνεται χρησιμοποιώντας μια ευρεία ποικιλία μέσων και μεθόδων. Η μεταφορά μπορεί να γίνεται με ηλεκτρονικά μέσα ή και σε μορφή εγγράφου μέσω ταχυδρομικής αποστολής.

Σε κάθε μεταφορά υπάρχει ο κίνδυνος απώλειας, υποκλοπής ή τυχαίας δημοσίευσης των πληροφοριών σε μη εξουσιοδοτημένα γι' αυτό άτομα.

Ο Δήμος έχει την υποχρέωση να φροντίζει για τη διαχείριση των πληροφοριών αυτών, για νομικούς λόγους, σύμφωνα και με το πνεύμα του νέου κανονισμού, αλλά και για τη διατήρηση της εμπιστοσύνης των συναλλασσομένων μαζί του, όπως επίσης είναι απαραίτητο η μεταφορά να πραγματοποιείται κατά τρόπο που να προστατεύει επαρκώς τις πληροφορίες.

Ο ρόλος του Δήμου σαν αποστολέας είναι να αξιολογήσει τους κινδύνους και να διασφαλίσει την ύπαρξη κατάλληλων μέτρων προστασίας. Αυτή η πολιτική περιγράφει τις ευθύνες και τις ελάχιστες απαιτήσεις ασφάλειας για την ασφαλή μεταφορά των πληροφοριών αυτών.

10.2 Σκοπός

Αυτή η πολιτική ορίζει τις ελάχιστες απαιτήσεις ασφαλείας για τη φυσική μεταφορά πληροφοριών από και προς τον Δήμο, σε οποιαδήποτε μορφή.

Για τους σκοπούς του παρόντος εγγράφου, οι πληροφορίες αφορούν και τις πληροφορίες κειμένου (π.χ. έγγραφα, αναφορές και υπολογιστικά φύλλα) και τα ακατέργαστα μη μορφοποιημένα δεδομένα (π.χ. εξωτερικοί δίσκοι backup), σε οποιαδήποτε μορφή και σε οποιοδήποτε μέσο, ηλεκτρονικό ή μη.

Αυτή η πολιτική ισχύει για όλους τους υπαλλήλους του Δήμου, όπως και για κάθε τρίτο που επεξεργάζεται πληροφορίες του.

10.3 Εξαιρέσεις

Αυτή η πολιτική δεν καλύπτει τη μεταφορά πληροφοριών μέσω του εσωτερικού δικτύου του Δήμου, το οποίο έχει τους δικούς του ελέγχους ασφαλείας. Επίσης δεν καλύπτει τυχόν χρηματικές συναλλαγές που έχουν τις δικές τους ξεχωριστές απαιτήσεις ασφάλειας, ή συναλλαγές που υλοποιούνται σαν μέρος σύμβασης των οποίων οι όροι ασφάλειας καθορίζονται από το τρίτο μέρος.

10.4 Ορισμοί

ΠΑΡΑΛΗΠΤΗΣ: Κάθε φυσικό ή νομικό πρόσωπο το οποίο ζητά πληροφορίες από κάποια διεύθυνση του Δήμου. Μπορεί να είναι εξωτερικός συνεργάτης, κάποια εταιρεία ή κάποια άλλη διεύθυνση εντός του Δήμου.

ΑΠΟΣΤΟΛΕΑΣ: Είναι το φυσικό πρόσωπο το οποίο για λογαριασμό του Δήμου, ξεκινά την αποστολή της πληροφορίας. Θα πρέπει να έχει ήδη την εξουσιοδότηση της διεύθυνσης και την απαραίτητη γνώση ως προς το να διακρίνει την κατηγοριοποίηση της πληροφορίας και αν μπορεί αυτή να μεταδοθεί με τον επιλεγμένο τρόπο. Προσοχή πρέπει να δίνεται στην περίπτωση αναμετάδοσης μιας πληροφορίας από άτομο που δεν έχει την εξουσιοδότηση ή τη γνώση να διακρίνει την κρισιμότητά της. Όταν ο υπάλληλος δεν μπορεί να αποφασίσει για την πληροφορία θα πρέπει πάντα να συμβουλεύεται τον προϊστάμενό του, τον υπεύθυνο ασφαλείας ή τον πρώτο αποστολέα της πληροφορίας.

10.5 Ρόλοι και Αρμοδιότητες

Οι κατάλληλοι ορισμοί των ρόλων και των ευθυνών είναι ουσιώδεις για τη διασφάλιση της συμμόρφωσης με την παρούσα πολιτική.

10.5.1 Αποστολέας

Ο αποστολέας είναι υπεύθυνος για την τήρηση των ακόλουθων απαιτήσεων της παρούσας πολιτικής:

- Για την αξιολόγηση των πληροφοριών που πρέπει να αποσταλούν.
- Για την εξασφάλιση της επίσημης επιβεβαίωσης της ταυτότητας και της εξουσιοδότησης λήψης του παραλήπτη
- Για τη λήψη της συγκατάθεσης του ιδιοκτήτη δεδομένων για τη μεταφορά.
- Για να εξασφαλίσει ότι οι πληροφορίες αποστέλλονται με τον πιο κατάλληλο τρόπο.

10.5.2 Υπεύθυνος Ασφάλειας

Ο Υπεύθυνος ασφαλείας θα πρέπει να παρακολουθεί και να ελέγχει τα τμήματα του Δήμου για να εξασφαλίσει τη συμμόρφωσή τους με όλες τις υποχρεωτικές και νομοκανονιστικές απαιτήσεις και τις εσωτερικές πολιτικές ασφαλείας.

10.5.3 Προϊστάμενοι τμημάτων

Οι διευθυντές των τμημάτων είναι υπεύθυνοι για τη διασφάλιση της διαθεσιμότητας της επικοινωνίας και της εφαρμογής αυτής της πολιτικής στο πλαίσιο της αρμοδιότητάς τους.

10.5.4 Υπάλληλοι

Οι υπάλληλοι είναι υπεύθυνοι ώστε να εξοικειωθούν με την παρούσα πολιτική και να εξασφαλίσουν ότι οποιαδήποτε μεταφορά πληροφοριών για την οποία είναι αυτοί υπεύθυνοι γίνεται κατά τρόπο συμβατό με την παρούσα πολιτική.

Οι υπάλληλοι πρέπει να αναφέρουν τυχόν ύποπτες ή πραγματικές παραβιάσεις ασφαλείας που σχετίζονται με τη μεταφορά δεδομένων άμεσα, στον Υπεύθυνο Ασφαλείας ή στον προϊστάμενό τους, σύμφωνα με τις διαδικασίες αντιμετώπισης συμβάντων ασφαλείας του Δήμου.

10.6 Αρμοδιότητες Αποστολέα

Σε κάθε μεταφορά υπάρχει ο κίνδυνος απώλειας, υποκλοπής ή τυχαίας δημοσίευσης των πληροφοριών σε μη εξουσιοδοτημένο άτομο. Είναι ευθύνη του αποστολέα να αξιολογήσει όλους τους κινδύνους και να εξασφαλίσει ότι είναι επαρκής οι έλεγχοι ασφάλειας και ότι συμμορφώνονται με την παρούσα πολιτική. Αυτή η ενότητα περιέχει ορισμένα από τα απαιτούμενα που πρέπει να ισχύουν πριν από τη μεταφορά των πληροφοριών.

10.7 Νομιμότητα και Αναγκαιότητα Μεταφοράς

Είναι επικίνδυνο να υποθέσουμε ότι επειδή κάποιος ζητά πληροφορίες είναι απαραίτητα και εξουσιοδοτημένος ή νομίμως δικαιούται να τις έχει. Αν υπάρχουν αμφιβολίες για τον παραλήπτη τότε πρέπει να ενημερώνετε άμεσα η διοίκηση ή ο υπεύθυνος ασφάλειας πληροφοριών.

Μόλις επιβεβαιωθεί ότι η μεταφορά είναι νόμιμη και απαραίτητη, τότε πρέπει να αποφασιστεί τι επιπέδου διαβάθμισης είναι η πληροφορία που θα αποσταλεί. Αυτό θα καθορίσει ποιο επίπεδο ασφάλειας είναι το κατάλληλο για το συγκεκριμένο τρόπο μεταφοράς.

Η μεταφορά προσωπικών ή εμπιστευτικών πληροφοριών χωρίς ελέγχους ασφαλείας μπορεί να αφήσει τον Δήμο έκθετο σε νομικά θέματα και να βλάψει τη φήμη του.

10.8 Προσωπικά Δεδομένα

Τα προσωπικά δεδομένα αφορούν ένα ζωντανό, αναγνωρίσιμο άτομο. Εάν περιέχονται μέσα σε αυτά και στοιχεία φυλετικής ή εθνοτικής καταγωγής, πολιτικές απόψεις, θρησκευτικές πεποιθήσεις, συνδικαλιστική συμμετοχή, δεδομένα σωματικής ή ψυχικής υγείας, σεξουαλικές προτιμήσεις, ή η διάπραξη αδικημάτων, χαρακτηρίζονται περαιτέρω ως ευαίσθητα προσωπικά δεδομένα.

Πριν την εκτέλεση οποιασδήποτε μεταφοράς θα πρέπει:

- Να υπάρχει τεκμηριωμένη η έγκριση του υπεύθυνου επεξεργασίας για τη συγκεκριμένη μεταφορά.
- Να επιβεβαιωθεί ότι η μεταφορά είναι σύμφωνη με τις νομοκανονιστικές απαιτήσεις και ιδιαίτερα σύμφωνη με τον ΓΚΠΔ.
- Να επιβεβαιωθεί ότι η μεταφορά είναι απαραίτητη.
- Να υπάρχει προηγούμενη σύμβαση με τον παραλήπτη, στην οποία θα πρέπει να αποτυπώνεται ότι κατανοεί τις ευθύνες του από τη στιγμή που θα λάβει στα συστήματά του πληροφορία που αφορά προσωπικά δεδομένα.

10.9 Εμπιστευτικά Δεδομένα

Οι εμπιστευτικές πληροφορίες είναι εκείνες τις οποίες ο Δήμος είναι υπεύθυνος να τηρεί με ασφάλεια. Αυτές μπορεί να περιλαμβάνουν πληροφορίες που επηρεάζουν τα επιχειρηματικά συμφέροντα ενός τρίτου ή πληροφορίες για τις οποίες ο αποστολέας δεν κατέχει πνευματικά δικαιώματα π.χ. τραπεζικές λεπτομέρειες, στοιχεία μισθών, συμβάσεις, συμφωνίες κλπ.

Η διαρροή τέτοιων πληροφοριών μπορεί να βλάψει τη φήμη του Δήμου ή και να επιφέρει νομικές συνέπειες.

Πριν την εκτέλεση οποιασδήποτε μεταφοράς θα πρέπει:

- Να υπάρχει τεκμηριωμένη η έγκριση του υπεύθυνου επεξεργασίας για τη συγκεκριμένη μεταφορά
- Να επιβεβαιώσετε ότι δεν παραβιάζετε η ευθύνη τήρησης της πληροφορίας με ασφάλεια

- Να επιβεβαιωθεί ότι η μεταφορά είναι απαραίτητη.
- Να αφαιρείται οτιδήποτε δεν είναι απαραίτητο για το σκοπό του παραλήπτη
- Να υπάρχει προηγούμενη σύμβαση με τον παραλήπτη, που να αποτυπώνεται ότι κατανοεί τις ευθύνες του από τη στιγμή που θα λάβει στα συστήματά του πληροφορία που αφορά προσωπικά δεδομένα.

10.10 Απαιτήσεις μεταφοράς Προσωπικών ή εμπιστευτικών δεδομένων

Αφού αποφασιστεί τι είδους πληροφορίες θα αποσταλούν και είναι έτοιμες για μετάδοση, ο αποστολέας πρέπει να εξετάσει τις διάφορες διαθέσιμες μεθόδους μεταφοράς και κατά πόσον αυτές είναι κατάλληλες.

Αυτή η ενότητα περιλαμβάνει τις κύριες μεθόδους αποστολής και καθορίζει τους περιορισμούς και τις απαιτήσεις για ασφαλή μεταφορά δεδομένων προσωπικού ή εμπιστευτικού χαρακτήρα.

Για όλες τις μεταβιβάσεις προσωπικών ή εμπιστευτικών δεδομένων, είναι απαραίτητο να έχει πιστοποιηθεί η ταυτότητα του παραλήπτη και να έχει πιστοποιηθεί κατάλληλα από τον αποστολέα.

10.11 Ηλεκτρονική Αλληλογραφία

Όπως αναφέρονται στην πολιτική ασφαλούς μετάδοσης μηνύματος ηλεκτρονικής αλληλογραφίας του Δήμου (Π.11).

10.12 Δικτυακή Μεταφορά (FTP, SecureFTP , VPN)

Το τυπικό πρωτόκολλο μεταφοράς αρχείων (FTP) χωρίς κρυπτογράφηση είναι εγγενώς ανασφαλές και δεν πρέπει να χρησιμοποιείται για τη μετάδοση προσωπικών ή εμπιστευτικών δεδομένων.

Οι μεταφορές αρχείων μέσω ασφαλούς πρωτοκόλλου μεταφοράς αρχείων (SFTP) είναι αποδεκτές, αλλά αυτές οι μεταφορές πρέπει να ρυθμίζονται και να διαχειρίζονται από το τμήμα πληροφορικής.

Για την περίπτωση της απομακρυσμένης σύνδεσης μέσω VPN, ακολουθείται η πολιτική τηλε-εργασίας (Π.02) του Δήμου.

10.13 Αφαιρούμενο Μέσο (CD, USB δίσκος, Κάρτα Μνήμης κλπ.)

Όπως αναφέρονται στην πολιτική χρήσης φορητών μέσων του Δήμου (Π.04).

10.14 Μετάδοση FAX

Το FAX είναι εγγενώς ανασφαλές και δεν συνιστάται για τη μεταφορά διαβαθμισμένων πληροφοριών. Ωστόσο, αναγνωρίζεται ότι ορισμένες περιστάσεις το απαιτούν. Σε αυτές τις περιπτώσεις θα πρέπει να ακολουθούνται τα παρακάτω:

- Ο αποστολέας πρέπει να ελέγξει ότι ο αριθμός φαξ είναι σωστός και ότι ο παραλήπτης περιμένει τη μετάδοση.
- Για πληροφορίες υψηλής ευαισθησίας, ο αριθμός πρέπει να ελέγχεται και από έναν άλλο συνάδελφο και εκτός της μετάδοσης να υπάρχει και τηλεφωνική επαφή με τον παραλήπτη καθ' όλη τη διάρκεια της αποστολής, για επιβεβαίωση της λήψης .
- Τόσο ο αποστολέας όσο και ο παραλήπτης θα πρέπει να έχουν μια συμφωνημένη διαδικασία για να αποφευχθεί η παραμονή του αντιγράφου στη μνήμη του μηχανήματος FAX και μια σαφή απαίτηση για την ασφαλή καταστροφή του μηνύματος όταν αυτό δεν απαιτείται πλέον.
- Το μήνυμα πρέπει να περιέχει σαφείς οδηγίες σχετικά με τις ευθύνες του παραλήπτη, αν αυτός δεν είναι τελικά ο σωστός παραλήπτης.
- Κάθε αποστολή θα πρέπει να επιβεβαιώνεται ότι λήφθηκε από τον σωστό παραλήπτη.

10.15 Ταχυδρομική ή με courier Αποστολή

Είναι σημαντικό ότι ο φάκελος, είτε περιέχει ηλεκτρονικό μέσο είτε χαρτί, πρέπει να διατηρείται ασφαλής κατά τη μεταφορά του και να παραδοθεί στο σωστό άτομο. Αυτό μπορεί να επιτευχθεί ακολουθώντας τις παρακάτω οδηγίες:

- Πρέπει να χρησιμοποιείται ένας αξιόπιστος μεταφορέας για την παράδοση.
- Το πακέτο θα πρέπει να συσκευάζεται με ασφάλεια, να φέρει σαφή ετικέτα και να φέρει σφραγίδα, η οποία θα πρέπει να σπάσει για να ανοίξει η συσκευασία.
- Το πακέτο πρέπει να έχει διεύθυνση επιστροφής και στοιχεία επικοινωνίας.

- Η ετικέτα δεν πρέπει να αναφέρει τη φύση ή την αξία των περιεχομένων.
- Το πακέτο πρέπει να παραδοθεί μόνο στον παραλήπτη και να υπογράψει ο ίδιος για την παραλαβή του.
- Ο αποστολέας πρέπει να ελέγξει άμεσα ότι η παράδοση ήταν επιτυχής.

10.16 Τηλεφωνική Μετάδοση

Καθώς οι τηλεφωνικές κλήσεις μπορεί να παρακολουθούνται, να ακούγονται (ανοικτή ακρόαση), να καταγράφονται ή να παρεμποδίζονται είτε σκόπιμα είτε τυχαία, πρέπει να ληφθούν μέτρα ασφάλειας, όπως παρακάτω:

- Οι πληροφορίες που μεταφέρονται πρέπει να περιορίζονται στο ελάχιστο.
- Οι προσωπικές ή εμπιστευτικές πληροφορίες δεν πρέπει να μεταφέρονται μέσω τηλεφώνου παρά μόνο όταν η ταυτότητα και η έγκριση του παραλήπτη έχει επιβεβαιωθεί.

10.17 SMS, Μηνύματα Κοινωνικών Δικτύων, Εφαρμογές Άμεσων Μηνυμάτων (Instant Messaging)

Δεν επιτρέπεται η μετάδοση εμπιστευτικών ή προσωπικών πληροφοριών με κανένα από τα παραπάνω μέσα, καθώς και τα ομοειδή αυτών.

10.18 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ

Ο Δήμος αναγνωρίζει την ευθύνη του να επεξεργάζεται τις πληροφορίες σωστά, σύμφωνα με όλες τις νομοκανονιστικές απαιτήσεις και τις απαιτήσεις των εσωτερικών πολιτικών ασφαλείας του.

Είναι ευθύνη του αποστολέα να αξιολογεί τον κίνδυνο αναλόγως της μεταφοράς που σκοπεύει να πραγματοποιήσει και να εξασφαλίσει ότι όλοι οι σχετιζόμενοι κίνδυνοι κατανοούνται και καλύπτονται επαρκώς και ότι η μεταφορά είναι κατάλληλα εγκεκριμένη βάσει των πολιτικών του Δήμου. Οι απαιτήσεις ασφάλειας για τις διάφορες μεθόδους αποστολής έχουν παρατεθεί στην παράγραφο 11.5 της παρούσας πολιτικής.

Ο Υπεύθυνος Ασφαλείας Δεδομένων είναι αρμόδιος για την εφαρμογή αυτής της πολιτικής.

10.19 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

α) Πολιτική χρήσης φορητών μέσων (Π.04)

β) Πολιτική τήλε-εργασίας (Π.02)

10.20 ΑΡΧΕΙΑ

Ουδέν

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ

11 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΟΥΣ ΑΠΟΣΤΟΛΗΣ E-Mail

11.1 ΣΚΟΠΟΣ

Σκοπός των παρόντων κανόνων ασφάλειας είναι να καθοριστεί, ο ασφαλής τρόπος χρήσης της υπηρεσίας μηνυμάτων ηλεκτρονικού ταχυδρομείου.

11.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Οι παρόντες κανόνες ασφάλειας εφαρμόζονται σε κάθε περίπτωση επικοινωνίας της Διεύθυνσης, τόσο εσωτερικά όσο και εξωτερικά, με αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου.

11.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Υπεύθυνος Ασφάλειας της Πληροφορίας
- Όλοι οι εργαζόμενοι

11.4 ΠΕΡΙΓΡΑΦΗ

11.4.1 Παραδοχές

12.4.1.1 Λαμβάνεται ως δεδομένο ότι η επικοινωνία με τους εξυπηρετητές e-mail γίνεται με τη χρήση ασφαλών πρωτοκόλλων SSL/TLS.

11.5 ΚΑΝΟΝΕΣ ΑΠΟΣΤΟΛΗΣ

12.5.2.1 Ο χρήστης είναι υπεύθυνος για την ορθή συμπλήρωση της σωστής διεύθυνσης του/των παραλήπτη/ών.

12.5.2.2 Απαγορεύεται να αναφέρονται στο πεδίο του τίτλου του μηνύματος ή/και στο σώμα του κειμένου του μηνύματος πληροφορίες που αφορούν σε δεδομένα της διεύθυνσης είτε σε προσωπικά δεδομένα.

12.5.2.3 Αν στο μήνυμα πρόκειται να αναφερθούν προσωπικά δεδομένα, αυτά θα πρέπει να εισάγονται πρώτα σε αρχείο (txt, xls, rtf, doc κλπ) και το αρχείο να μεταδίδεται σαν συνημμένο.

12.5.2.4 Αν στο μήνυμα πρόκειται να αναφερθούν ευαίσθητα προσωπικά δεδομένα δεν θα μεταδίδονται αν το συνημμένο αρχείο δεν είναι προστατευμένο, τουλάχιστον με κωδικό πρόσβασης ή κρυπτογράφηση.

11.6 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ

Οποιοσδήποτε εργαζόμενος παραβιάσει την παρούσα Πολιτική Ασφάλειας μπορεί να υπόκειται σε πειθαρχικές κυρώσεις κατά την κρίση της Διοίκησης.

11.7 ΧΡΗΣΙΜΟΠΟΙΟΥΜΕΝΑ ΕΝΤΥΠΑ

ΟΥΔΕΝ

11.8 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ

12 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ B.Y.O.D. (Bring Your Own Device)

12.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγραφεί η μεθοδολογία διασύνδεσης προσωπικών υπολογιστών στο δίκτυο και στα υπολογιστικά συστήματα του Δήμου όπως επίσης και οι ελάχιστες απαιτήσεις ασφαλείας που θα πρέπει να τηρούνται από τους ιδιοκτήτες των υπολογιστών αυτών .

12.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται για όλα τα μέσα που δύνανται να συνδέονται στο εταιρικό δίκτυο, ήτοι φορητοί υπολογιστές (laptops), κινητά τηλέφωνα, tablets κλπ.

12.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Υπεύθυνος Προστασίας Δεδομένων

- IT
- Ιδιοκτήτες πόρων

12.4 ΠΕΡΙΓΡΑΦΗ

12.4.1 Χρήση Συσκευών

12.4.1.1. Γενικοί Κανόνες

Απαγορεύεται η χρήση μη εξουσιοδοτημένων/εγκεκριμένων φορητών υπολογιστών και/ή άλλων συσκευών όπως περιγράφονται παραπάνω. Η χρήση μπορεί να εκτελείται μόνο από εγκεκριμένες από τη Διεύθυνση Πληροφορικής του Δήμου συσκευές. Μετά την έγκριση χρήσης οποιασδήποτε συσκευής, δεν επιτρέπεται να γίνουν τροποποιήσεις και εγκαταστάσεις νέων προγραμμάτων χωρίς την προηγούμενη άδεια της Διεύθυνσης Πληροφορικής. Οι συσκευές θα πρέπει να ελέγχονται ανά τακτά χρονικά διαστήματα από την Διεύθυνση Πληροφορικής.

12.4.1.2.Εγγραφή στο Μητρώο

Οι συσκευές BYOD δεν εγγράφονται στο μητρώο συσκευών του Δήμου αλλά στη λίστα συσκευών του Μέρους Γ'. Κατ' ελάχιστο θα πρέπει να αναφέρονται ο κάτοχος της συσκευής, ο σειριακός αριθμός της, το όνομα υπολογιστή, η Διεύθυνση του Δήμου όπου χρησιμοποιείται και τα επιπλέον εγκεκριμένα προγράμματα που έχουν εγκατασταθεί.

12.4.1.3. Ευθύνη Τεχνικής Υποστήριξης

Η Διεύθυνση Πληροφορικής διατηρεί το δικαίωμα, χωρίς να είναι υποχρεωμένη να ενημερώσει πρώτα τον χρήστη, να διακόψει και/'η να απαγορεύσει τη σύνδεση συσκευής στο δίκτυο εάν επηρεάζονται θέματα ασφαλείας του δικτύου.

12.5 Ασφάλεια Συσκευής

12.5.1 Ρυθμίσεις συσκευής

Για να μπορεί να συνδεθεί μια συσκευή στο δίκτυο του Δήμου, θα πρέπει η συσκευή να ελεγχθεί πρώτα από τη Διεύθυνση Πληροφορικής για να πιστοποιηθεί ότι καλύπτει ορισμένα ελάχιστα κριτήρια ασφάλειας.

12.5.2 Ελάχιστα κριτήρια ασφάλειας

Σαν ελάχιστα κριτήρια ασφάλειας ορίζονται τα παρακάτω:

Α. Λειτουργικό σύστημα

Windows 10, έκδοση 1809 και νεότερη
Android έκδοση 6.0 (Marshmallow) ή iOS έκδοση 10.3.3 για κινητές συσκευές

Β. Ισχυρός κωδικός log-in χρήστη

Γ. Εγκατεστημένο πρόγραμμα antivirus

Δ. Ενεργό firewall (μόνο για υπολογιστές)

Ε. Προφίλ χρήστη (για χρήση μόνο για εργασία στον Δήμο)

12.5.3 Εγκεκριμένα Προγράμματα

12.5.3.1 Για την εξασφάλιση της σύνδεσης θα πρέπει η συσκευή να έχει εγκατεστημένα μόνο προγράμματα όπως αυτά αναφέρονται στο Μέρος Α’, (Λίστα Εγκεκριμένων Προγραμμάτων).

12.5.3.2. Εάν απαιτείται η εγκατάσταση και χρήση προγραμμάτων που δεν αναφέρονται στη λίστα εγκεκριμένων προγραμμάτων θα πρέπει να γίνεται αίτημα προς τη Διεύθυνση Πληροφορικής, ώστε να εξεταστεί κατά πόσο το πρόγραμμα πληρεί τους όρους ασφάλειας της πολιτικής ασφαλείας της διεύθυνσης όπου θα χρησιμοποιηθεί η συσκευή και σε περίπτωση

θετικής έκβασης του ελέγχου, το συγκεκριμένο πρόγραμμα να συμπεριληφθεί στο Μέρος Β' (Λίστα Πρόσθετων Εγκεκριμένων Προγραμμάτων).

12.5.3.3. Όλα τα προγράμματα των παραπάνω παραγράφων θα πρέπει να συνοδεύονται από πιστοποιητικό γνησιότητας, να υπάρχουν σε ισχύ οι απαιτούμενες άδειες χρήσης και να είναι ενημερωμένα στην τελευταία διαθέσιμη έκδοση.

12.6 Τεχνική Υποστήριξη

Η τεχνική υποστήριξη των συσκευών που εμπίπτουν στην παρούσα πολιτική από πλευράς Διεύθυνσης Πληροφορικής περιορίζεται μόνο σε επίλυση θεμάτων σύνδεσης με το δίκτυο. Κάθε άλλο τεχνικό πρόβλημα αποτελεί ευθύνη του ιδιοκτήτη της συσκευής.

12.7 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ

- Παράρτημα ΙΙ.1 – Λίστα Εγκεκριμένων Προγραμμάτων
- Παράρτημα ΙΙ.2 – Λίστα Πρόσθετων Εγκεκριμένων Προγραμμάτων
- Μέρος Γ' – Μητρώο Συσκευών BYOD

12.8 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
1. ΕΠ.05.02, Μητρώο συσκευών BYOD 2. Μέρος Α' παρούσης	Αρχείο excel Φυσικό Αρχείο		

Μέρος Α’

ΛΙΣΤΑ ΣΥΣΚΕΥΩΝ (BYOD)

Α/Α	Όνομα Κατόχου	Σειριακός Συσκευής	Όνομα Υπολογιστή	Γραφείο Υπαλλήλου	Επιπλέον Προγράμματα

13 ΠΟΛΙΤΙΚΗ ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗΣ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΕΔΟΜΕΝΩΝ

Τα σχετικά με αυτή την πολιτική διέπονται από τον Κανονισμό Επικοινωνίας Δημοσίων Υπηρεσιών του Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης.

Για σκοπούς εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων και σε αντιστοιχία με τον κανονισμό αλληλογραφίας δημοσίων υπηρεσιών, σαν «Αδιαβάθμητα» ή «Κοινά» νοούνται συστήματα χωρίς προσωπικά δεδομένα, σαν «Εμπιστευτικά» συστήματα με απλά προσωπικά δεδομένα και σαν «Απόρρητα» συστήματα με ευαίσθητα προσωπικά δεδομένα.

14 ΠΟΛΙΤΙΚΗ ΤΗΛΕΔΙΑΣΚΕΨΕΩΝ

14.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγραφεί η μεθοδολογία διασύνδεσης από απομακρυσμένους υπολογιστές στο εσωτερικό δίκτυο και στα υπολογιστικά συστήματα του οργανισμού για σκοπούς τηλεργασίας και να περιγράψει τις μεθόδους και τις εφαρμογές οι οποίες μπορούν να χρησιμοποιηθούν για την εκτέλεση τηλεδιασκέψεων με το προσωπικό ή/και εξωτερικούς συνεργάτες ή/και πελάτες του οργανισμού.

14.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε όλο το προσωπικό για όλα τα μέσα που χρησιμοποιούνται για τηλεργασία και δύνανται να συνδέονται στο εσωτερικό δίκτυο ή / και

δύνανται να χρησιμοποιούνται για την εκτέλεση μίας τηλεδιάσκεψης, ήτοι σταθεροί υπολογιστές (desktops), φορητοί υπολογιστές (laptops), κινητά τηλέφωνα, tablets κλπ.

14.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Υπεύθυνος Προστασίας Δεδομένων
- Υπεύθυνος Τμήματος Πληροφορικής
- Εργαζόμενοι

14.4 ΠΕΡΙΓΡΑΦΗ

14.4.1 Τηλεργασία – Χρήση Συσκευών

Η εκτέλεση τηλεργασίας ή / και τηλεδιασκέψεων μπορεί να γίνεται από συσκευές που προμηθεύει ο οργανισμός για το σκοπό αυτό στους χρήστες ή από προσωπικές συσκευές των χρηστών, αφού πρώτα ελεγχθούν και εγκριθούν από το Τμήμα Πληροφορικής.

Απαγορεύεται η χρήση μη εξουσιοδοτημένων / εγκεκριμένων υπολογιστών και / ή άλλων συσκευών. Μετά την έγκριση χρήσης οποιασδήποτε συσκευής, δεν επιτρέπεται να γίνουν τροποποιήσεις και εγκαταστάσεις νέων προγραμμάτων χωρίς την προηγούμενη άδεια του Τμήματος Πληροφορικής. Οι εξουσιοδοτημένες συσκευές μπορεί να ελέγχονται ανά τακτά χρονικά διαστήματα από το Τμήμα Πληροφορικής.

14.4.2 Ρυθμίσεις Ασφάλειας Συσκευής

Για να μπορεί να συνδεθεί μια συσκευή απομακρυσμένα στο εσωτερικό δίκτυο με την υλοποίηση της τεχνολογίας VPN (Virtual Private Network), θα πρέπει η συσκευή να ελεγχθεί από το Τμήμα Πληροφορικής ότι καλύπτει ορισμένα ελάχιστα κριτήρια ασφάλειας.

Σαν ελάχιστα κριτήρια ασφάλειας ορίζονται τα παρακάτω:

Α. Λειτουργικό σύστημα:

Windows 10, έκδοση 1809 και νεότερη
Android έκδοση 6.0 (Marshmallow) ή iOS έκδοση 10.3.3 για κινητές συσκευές

Β. Ισχυρός κωδικός log-in χρήστη, όπως προβλέπεται από την Πολιτική Απορρήτου Κωδικών Χρηστών.

Γ. Εγκατεστημένο και ενημερωμένο πρόγραμμα antivirus

Δ. Ενεργό firewall (μόνο για υπολογιστές)

Ε. Λογαριασμός Χρήστη με προστασία κωδικού πρόσβασης

14.4.3 Ρυθμίσεις Ασφαλείας Σύνδεσης

Η απομακρυσμένη σύνδεση πρέπει να είναι καλύπτει όλες τις προδιαγραφές ασφαλείας. Για την εξασφάλιση της σύνδεσης θα πρέπει να ρυθμιστεί η επίτευξη της να υλοποιείται με την χρήση του ασφαλούς πρωτοκόλλου (π.χ. IPSec VPN). Επίσης, όπου είναι εφικτό, γίνεται χρήση ιδιωτικού / δημόσιου κλειδιού.

Επιτρέπεται η σύνδεση σε υπολογιστικά συστήματα του Οργανισμού μέσω υπηρεσίας «απομακρυσμένης επιφάνειας εργασίας» (Remote Desktop Protocol), μόνο όταν αυτή γίνεται μέσω ασφαλούς εικονικού ιδιωτικού δικτύου (VPN).

Με τη χρήση της VPN τεχνολογίας σε προσωπικό εξοπλισμό, οι χρήστες θα πρέπει να κατανοήσουν ότι τα μηχανήματα που χρησιμοποιούν για την πραγματοποίηση της σύνδεσης τους, καθίστανται προέκταση του δικτύου του οργανισμού. Συνέπεια τούτου είναι ότι πρέπει να ακολουθούν τις πολιτικές ασφαλείας του οργανισμού και ο ιδιωτικός εξοπλισμός τους υπόκειται στους ίδιους κανόνες που εφαρμόζονται για τον εξοπλισμό του οργανισμού.

14.5 Τηλεργασία – Υπευθυνότητες

Για την εκτέλεση τηλεργασίας θα πρέπει να εξασφαλίζεται ότι ακολουθούνται οι παρακάτω όροι και κανόνες τόσο από το Τμήμα Πληροφορικής του οργανισμού, όσο και από τους χρήστες.

14.5.1 Τμήμα Πληροφορικής

- Παρέχει κάθε δυνατή βοήθεια και εκπαίδευση στους χρήστες σε θέματα απομακρυσμένης σύνδεσης στο εσωτερικό δίκτυο του οργανισμού.

- Εξασφαλίζει ότι οι χρήστες που εκτελούν τηλε-εργασία περιορίζονται στους ελάχιστους απαραίτητους με βάση τα καθήκοντά τους και οι προσβάσεις τους είναι οι ελάχιστες απαραίτητες, για την εκτέλεση των καθηκόντων τους, σύμφωνα με την υφιστάμενη Πολιτική Προσβάσεων του οργανισμού.

- Εξασφαλίζει την δυνατότητα κρυπτογράφησης των αρχείων που μπορεί να αποθηκευτούν στη συσκευή του χρήστη από την οποία θα εκτελείται η τηλε-εργασία (laptop, desktop, tablet) ή σε αφαιρούμενο μέσο (π.χ. usb sticks) ή υπηρεσία διαδικτυακής αποθήκευσης (π.χ. Dropbox, One Drive, Google Drive, κλπ), σύμφωνα με την Πολιτική Χρήσης Αφαιρούμενων Μέσων του οργανισμού.

- Αξιολογεί και όπου είναι τεχνικά εφικτό, παρέχει στους ασκούντες τηλε-εργασία τη δυνατότητα χρήσης της επαγγελματικού ταχυδρομείου (email) για αποστολή ή λήψη μηνυμάτων για σκοπούς τηλεργασίας από εξωτερικό δίκτυο.

- Φροντίζει για τη λήψη αντιγράφων ασφαλείας για αρχεία με προσωπικά δεδομένα, τα οποία υφίστανται επεξεργασία στο πλαίσιο δραστηριοτήτων τηλεργασίας με βάση την Πολιτική Αντιγράφων Ασφαλείας.

14.5.2 Χρήστες Τηλεργασίας

Με την βοήθεια και τις συμβουλές του Τμήματος Πληροφορικής του οργανισμού, οι χρήστες θα πρέπει να εξασφαλίζουν και να μεριμνούν για τα παρακάτω:

- Την εγκατάσταση αντιϊκού προγράμματος και την καθημερινή του ενημέρωση, όπως και την ενεργοποίηση και λειτουργία του firewall της συσκευής τους.

- Ο σταθμός εργασίας να συνδέεται στον εξοπλισμό του παρόχου internet, που διαθέτει ο χώρος, μέσω καλωδίου δικτύου. Εάν αυτό δεν είναι εφικτό, και πρέπει να συνδέεται στο διαδίκτυο μέσω ασύρματου δικτύου, θα πρέπει να ρυθμιστεί κατάλληλα ο εξοπλισμός του παρόχου, ώστε να χρησιμοποιεί το πρωτόκολλο ασφαλείας WPA2 και ισχυρό κωδικό πρόσβασης.

- Την εγκατάσταση των τελευταίων διαθέσιμων ενημερώσεων του λειτουργικού συστήματος και των εφαρμογών του υπολογιστή τους.

- Την χρήση προγραμμάτων πλοήγησης στο διαδίκτυο (π.χ. Microsoft Edge, Google Chrome, Mozilla Firefox κλπ) με ανώνυμη περιήγηση ή τη διαγραφή από το ιστορικό των συνδέσμων που σχετίζονται με την τηλεργασία τους.

- Αποφυγή χρήσης προσωπικού ηλεκτρονικού ταχυδρομείου (π.χ. gmail, yahoo, hotmail) για αποστολή ή λήψη μηνυμάτων για σκοπούς τηλεργασίας. Αντί αυτού, θα πρέπει να χρησιμοποιείται η επαγγελματική ηλεκτρονική διεύθυνση την οποία παρέχει ο Οργανισμός. Εάν αυτό δεν είναι τεχνικά εφικτό, τότε το περιεχόμενο των μηνυμάτων που αφορά προσωπικά δεδομένα πρέπει να κρυπτογραφείται κατάλληλα (π.χ. είτε ολόκληρο το μήνυμα είτε μόνο τα συνημμένα αρχεία).

- Αποφυγή χρήσης εφαρμογών ανταλλαγής μηνυμάτων (κείμενο ή/και βίντεο) για τους σκοπούς της τηλεργασίας από υπηρεσίες των οποίων τα χαρακτηριστικά ασφάλειας (κρυπτογράφηση, ρυθμίσεις προστασίας δεδομένων) αξιολογούνται ως μη ισχυρά.

- Αποφυγή αποθήκευσης αρχείων σε τοπικό υπολογιστή ή υπηρεσία διαδικτυακής αποθήκευσης (π.χ. Dropbox, One Drive, Google Drive, κλπ). Αν αυτό δεν είναι εφικτό, προστασία τουλάχιστον με κωδικό πρόσβασης των αποθηκευμένων αρχείων της εργασίας τους ή την κρυπτογράφησή τους, ιδιαίτερα αν τα αρχεία αυτά περιέχουν προσωπικά δεδομένα.

- Την αποθήκευση των αρχείων που χρησιμοποιούν για την τηλεργασία, σε διακριτούς φακέλους, διαφορετικούς από αυτούς που χρησιμοποιούν για τα προσωπικά τους αρχεία.

- Τη λήψη αντίγραφου ασφαλείας των αρχείων με προσωπικά δεδομένα, σύμφωνα με τις οδηγίες του τμήματος πληροφορικής του οργανισμού.

- Εφαρμογή της Πολιτικής Καθαρής Οθόνης στις συσκευές που χρησιμοποιούνται για τηλεργασία με κλείδωμά τους (π.χ. προφύλαξη οθόνης, με κωδικό απενεργοποίησης) αν μείνουν ανενεργές.

14.6 Τηλεδιασκέψεις – Ασφάλεια Σύνδεσης

Ο χρήστης, από την απομακρυσμένη του θέση, καταβάλει κάθε προσπάθεια ώστε ο σταθμός εργασίας του να συνδέεται στον εξοπλισμό του παρόχου internet, που διαθέτει ο χώρος, μέσω καλωδίου δικτύου. Εάν αυτό δεν είναι εφικτό, και πρέπει να συνδέεται στο διαδίκτυο μέσω

ασύρματου δικτύου, θα πρέπει να ρυθμιστεί κατάλληλα ο εξοπλισμός του παρόχου, ώστε να χρησιμοποιεί το πρωτόκολλο ασφαλείας WPA2 και ισχυρό κωδικό πρόσβασης.

Η αποθήκευση αρχείων στον τοπικό υπολογιστή του χρήστη θα πρέπει να αποφεύγεται. Όλα τα αρχεία, τα οποία θα χρειαστεί να αποθηκευτούν τοπικά, θα πρέπει να προστατεύονται με κωδικό πρόσβασης ή να κρυπτογραφούνται.

14.7 Ασφάλεια Εφαρμογών Τηλεδιάσκεψης

Για τη επιλογή χρήσης συγκεκριμένης εφαρμογής εξετάζονται και εφαρμόζονται οι παρακάτω κανόνες για την προστασία των προσωπικών δεδομένων αλλά και των ευαίσθητων πληροφοριών του οργανισμού.

- Θα πρέπει η επιλεγμένη εφαρμογή να υποστηρίζει κρυπτογράφηση από άκρη σε άκρη (end-to-end encryption).
- Οι όροι χρήσης της επιλεγμένης εφαρμογής να καλύπτουν τις απαιτήσεις ασφαλείας του οργανισμού, όπως αυτές έχουν αποτυπωθεί στη γενική πολιτική ασφαλείας του οργανισμού.
- Ο σύνδεσμος μιας προγραμματισμένης τηλεδιάσκεψης δεν θα πρέπει να δημοσιοποιείται πουθενά, παρά μόνο να κοινοποιείται στους συμμετέχοντες.
- Κατά τη διάρκεια της τηλεδιάσκεψης, απαγορεύεται η καταγραφή της σε video, το οποίο μπορεί να αναπαραχθεί αργότερα, όπως απαγορεύεται και η λήψη στιγμιότυπων των συμμετεχόντων.

14.8 Εφαρμογές Τηλεδιάσκεψης

Το Τμήμα Πληροφορικής του Οργανισμού είναι αρμόδιο για την επιλογή και έγκριση των κατάλληλων εφαρμογών τηλεδιάσκεψης που καλύπτουν τις ανωτέρω προδιαγραφές. Δεν επιτρέπεται η χρήση μη εξουσιοδοτημένων/εγκεκριμένων εφαρμογών τηλεδιασκέψεων. Δεν επιτρέπεται η εγκατάσταση οποιασδήποτε εφαρμογής τηλεδιάσκεψης από τους χρήστες στους τοπικούς σταθμούς εργασίας τους χωρίς την προηγούμενη γραπτή έγκριση του τμήματος πληροφορικής.

14.9 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ

Οποιοσδήποτε εργαζόμενος παραβιάσει την παρούσα Πολιτική Ασφάλειας ενδέχεται να υποστεί πειθαρχικές κυρώσεις.

14.10 ΣΥΝΗΜΜΕΝΑ ΕΝΤΥΠΑ

- Ουδέν

14.11 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ

ΠΑΡΑΤΗΜΑ ΙΙ

Λίστα Προγραμμάτων

1 Εγκεκριμένα

Windows 10 Pro

Office 2016 Pro

Acrobat reader

7zip

Eset Antivirus

Skype

CDBurnXP

WinRar

Putty

CCleaner

Vmware Player

Chrome

Firefox

Vlc

Java

Teamviewer

GoogleEarth

MPC Home Cinema

Adobe Air

Adobe Flash

Adobe Shockwave

Adblock Plus

2 Πρόσθετα