ΔΗΜΟΣ ΚΙΛΚΙΣ

Πολιτική Διατήρησης και Προστασίας Δεδομένων

Data Retention and Security Policy

ΔΗΜΟΣ ΚΙΛΚΙΣ

Πολιτική Διατήρησης και Προστασίας Δεδομένων

Data Retention and Security Policy

Ταξινόμηση Εγγράφου:	**Εσωτερικό Έγγραφο**
Έγγραφο Ανάφ.	**GDPR-DOC-16**
Έκδοση:	1
Χρονολογημένο:	**29 Νοεμβρίου 2018**
Συντάκτης Εγγράφου:	**Proset I.K.E**

Ιστορικό Εγγράφου

Έκδοση	Ημερομηνία	Συντάκτης Αναθεώρησης	Σύνοψη αλλαγών

Έγκριση

Όνομα	Θέση	Υπογραφή	Ημερομηνία

Περιεχόμενα

Κατάλογος Πινάκων

1 Εισαγωγή

Στις καθημερινές υπηρεσιακές δραστηριότητές του, ο «Δήμος Κιλκίς» συλλέγει και αποθηκεύει πληροφορίες πολλών τύπων και σε διάφορες μορφές (έντυπα και ηλεκτρονικά). Η σχετική σημασία και ευαισθησία των εν λόγω πληροφοριών ποικίλλει και εξαρτάται από το σύστημα ταξινόμησης ασφαλείας του οργανισμού.

Είναι σημαντικό οι πληροφορίες να προστατεύονται από απώλεια, καταστροφή, πλαστογράφηση, μη εξουσιοδοτημένη πρόσβαση και μη εξουσιοδοτημένη δημοσιοποίηση. Μια σειρά ελέγχων και μέτρων χρησιμοποιούνται για να διασφαλιστεί αυτό, συμπεριλαμβανομένων των αντιγράφων ασφαλείας, του ελέγχου πρόσβασης και της κρυπτογράφησης. Τα προσωπικά δεδομένα αποτελούν μέρος των πληροφοριών που επεξεργάζεται ο «Δήμος Κιλκίς» τα οποία απαιτούν μεγαλύτερη ασφάλεια και ως εκ τούτου καθορίζουν και τον τελικό βαθμό αυστηρότητας της πολιτικής.
Με τον όρο «δεδομένα» στο εξής θα θεωρούμε τα προσωπικά δεδομένα αλλά και το σύνολο των πληροφοριών

Ο«Δήμος Κιλκίς» έχει επίσης την ευθύνη να διασφαλίζει ότι συμμορφώνεται με όλες τις σχετικές νομικές, ρυθμιστικές και συμβατικές απαιτήσεις στη συλλογή, αποθήκευση, ανάκτηση και καταστροφή των πληροφοριών. Ιδιαίτερη σημασία έχει ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) και οι απαιτήσεις του σχετικά με την αποθήκευση και επεξεργασία δεδομένων προσωπικού χαρακτήρα και στον οποίο ο «Δήμος Κιλκίς» θα πρέπει να συμμορφωθεί.

Αυτός ο έλεγχος ισχύει για όλα τα συστήματα, τους ανθρώπους και τις διαδικασίες που αποτελούν τα πληροφοριακά συστήματα του οργανισμού, συμπεριλαμβανομένων μελών του διοικητικού συμβουλίου, διευθυντών, υπαλλήλων, προμηθευτών και άλλων τρίτων που έχουν πρόσβαση στα συστήματα του «Δήμου Κιλκίς».

Για το παρόν έγγραφο ισχύουν οι ακόλουθες πολιτικές και διαδικασίες:

- *GDPR-DOC-17Πολιτική Προστασίας Απορρήτου και Προσωπικών Δεδομένων*
- *GDPR-DOC-13Απογραφή Στοιχείων Προσωπικών Δεδομένων*
- *GDPR-DOC-30 Οργανωτικά και Τεχνικά μέτρα ασφάλειας*

2 Πολιτική Διατήρησης και Ασφάλειας Δεδομένων

Αυτή η πολιτική ξεκινά με τη θέσπιση των βασικών αρχών που πρέπει να υιοθετηθούν κατά την εξέταση της διατήρησης και της προστασίας των Δεδομένων σε οποιοδήποτε μέσο αποθηκεύονται ή προβάλλονται και με οποιοδήποτε μέσο διακινούνται. Στη συνέχεια, καθορίζει τους τύπους δεδομένων που κατέχει ο «Δήμος Κιλκίς» και τις γενικές τους απαιτήσεις, και στην συνέχεια την προστασία, την καταστροφή και τη διαχείριση τους.

2.1 Γενικές Αρχές

Υπάρχουν ορισμένες βασικές γενικές αρχές που πρέπει να υιοθετηθούν κατά την εξέταση της πολιτικής διατήρησης και προστασίας των δεδομένων. Αυτά είναι:

- Η ασφάλεια των δεδομένων είναι ευθύνη όλων
- Τα δεδομένα πρέπει να κρατούνται σύμφωνα με όλες τις ισχύουσες νομικές, ρυθμιστικές και συμβατικές υποχρεώσεις
- Τα δεδομένα δεν πρέπει να κρατούνται για περισσότερο από όσο απαιτείται
- Η προστασία των δεδομένων όσον αφορά την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους πρέπει να είναι σύμφωνη με την ταξινόμηση ασφαλείας τους
- Τα δεδομένα πρέπει να παραμένουν ανακτήσιμα σύμφωνα με τις υπηρεσιακές απαιτήσεις ανά πάσα στιγμή
- Όπου ενδείκνυται, τα δεδομένα προσωπικού χαρακτήρα πρέπει να υπόκεινται το συντομότερο δυνατόν σε τεχνικές που να εμποδίζουν την ταυτοποίηση τους με ένα άτομο (ανωνυμοποίηση, ψευδοανωνυμοποίηση, κρυπτογράφηση).
- Τα πληροφοριακά συστήματα του «Δήμου Κιλκίς» παρέχονται για υπηρεσιακή χρήση.
- Η χρήση οποιουδήποτε συστήματος πληροφορικής του «Δήμου Κιλκίς» για προσωπικούς λόγους (συμπεριλαμβανομένου του ηλεκτρονικού ταχυδρομείου και του ιστού) επιτρέπεται μόνο σύμφωνα με τις οδηγίες αυτής της πολιτικής.
- Ο «Δήμος Κιλκίς» διατηρεί το δικαίωμα να παρακολουθεί τα πληροφοριακά συστήματα του, προκειμένου να προστατεύει τα νόμιμα υπηρεσιακά του συμφέροντα. Οι πληροφορίες που συλλέγονται από την παρακολούθηση αυτή μπορούν να χρησιμοποιηθούν για την υποκίνηση ή τη στήριξη πειθαρχικών διαδικασιών.

- Το προσωπικό εκπαιδεύεται τακτικά σε θέματα προστασίας προσωπικών δεδομένων και συμμόρφωσης στο GDPR, καθώς και σε ειδικά θέματα σχετικά με την ασφάλεια του πληροφοριακού συστήματος

2.2 Κατηγορίες Δεδομένων

Για να βοηθήσετε στον καθορισμό των οδηγιών για τη διατήρηση και την προστασία των δεδομένων, τα δεδομένα που τηρούνται από τον «Δήμο Κιλκίς» ομαδοποιούνται στις κατηγορίες που παρατίθενται στον πίνακα στην επόμενη σελίδα. Για καθεμία από αυτές τις κατηγορίες, δίνονται επίσης η απαιτούμενη ή συνιστώμενη περίοδος διατήρησης και τα επιτρεπόμενα μέσα αποθήκευσης, μαζί με έναν λόγο για τη σύσταση ή την απαίτηση.

Αυτές είναι μόνο κατευθυντήριες γραμμές και μπορεί να υπάρχουν συγκεκριμένες περιστάσεις όπου οι εγγραφές πρέπει να διατηρούνται για μεγαλύτερο ή βραχύτερο χρονικό διάστημα. Αυτό θα πρέπει να αποφασίζεται κατά περίπτωση, ως μέρος του σχεδιασμού των στοιχείων ασφάλειας των πληροφοριών από νέες ή σημαντικά μεταβαλλόμενες διαδικασίες και υπηρεσίες.

Περισσότερες πληροφορίες σχετικά με τις εγγραφές που κατέχει ο Δήμος, συμπεριλαμβανομένων των ταξινομήσεων ασφαλείας και των ιδιοκτητών τους, μπορούν να βρεθούν στην *GDPR-DOC-13Απογραφή Στοιχείων Προσωπικών Δεδομένων*.

Κατηγορία Δεδομένων	Περιγραφή	Περίοδος Διατήρησης	Λόγοι για την Περίοδο Διατήρησης	Επιτρεπόμενο Μέσο Αποθήκευσης
Λογιστικής	Τιμολόγια, εντολές αγοράς, λογαριασμοί και άλλα ιστορικά οικονομικές εγγραφές	10 χρόνια	Απαίτηση συμμόρφωσης με την νομοθεσία	Έντυπα/ηλεκτρονικά
Backup βάσεων δεδομένων	Περιοδικά backup βάσεων δεδομένων και άλλες εγγραφές καταγραφής που χρησιμοποιούνται για την ανάκτηση βάσεων δεδομένων	x εβδομάδες	Βασίζεται στη στρατηγική δημιουργίας αντιγράφων ασφαλείας και αποκατάστασης	Ηλεκτρονικά / μέσα μαγνητοταινίας/DVD
Προμηθευτών	Ονόματα προμηθευτών, διευθύνσεις, στοιχεία της εταιρείας	10 χρόνια	Μέγιστη περίοδος εντός της οποίας μπορεί να προκύψει κάποια διαφορά	Ηλεκτρονικά / Έντυπα /
Ανθρώπινου Δυναμικού	Όνομα υπαλλήλων, διευθύνσεις, τραπεζικά στοιχεία, φορολογικοί κωδικοί, ιστορικό απασχόλησης	x χρόνια μετά το τέλος της απασχόλησης	Υποχρέωση προστασίας δεδομένων Νόμος περί απασχόλησης	Ηλεκτρονικά / Έντυπα
Συμβάσεις	Ονοματεπώνυμο, Διεύθυνση, οικονομικά στοιχεία	x χρόνια από τη λήξη της σύμβασης	Μέγιστη περίοδος εντός της οποίας μπορεί να προκύψει διένεξη	Ηλεκτρονικά / Έντυπα

Πίνακας1–Τύποι Εγγραφών και περίοδοι διατήρησης

2.3 Διαχείριση επικοινωνιών και λειτουργιών

2.3.1 Σχεδιασμός και αποδοχή συστήματος

Όλες οι συνιστώσες ή οι εγκαταστάσεις υποδομής πληροφορικής του «Δήμου Κιλκίς» καλύπτονται από στρατηγικές σχεδιασμού και αντικατάστασης χωρητικότητας για να διασφαλιστεί ότι οι αυξημένες απαιτήσεις για την περισσότερη δύναμη και αποθήκευση δεδομένων μπορούν να αντιμετωπιστούν και να εκπληρωθούν έγκαιρα.

Βασικά συστατικά στοιχεία υποδομής πληροφορικής περιλαμβάνουν, χωρίς να περιορίζονται σε αυτά, τα ακόλουθα:

- Διακομιστές
- Διαγνωστικά μηχανήματα,
- Προσωπικοί υπολογιστές
- Εκτυπωτές
- Δίκτυα
- Περιβαλλοντικοί έλεγχοι συμπεριλαμβανομένου του κλιματισμού

Τα νέα συστήματα πληροφορικής, οι αναβαθμίσεις προϊόντων και οι ενημερώσεις κώδικα πρέπει να υποβάλλονται σε κατάλληλο επίπεδο ελέγχου πριν από την αποδοχή και την παραγωγική τους λειτουργία.

Τα κριτήρια αποδοχής πρέπει να είναι σαφώς προσδιορισμένα, να συμφωνούνται και να τεκμηριώνονται και να περιλαμβάνουν την άδεια διαχείρισης.

Τα λειτουργικά συστήματα, και οι εφαρμογές τρίτου μέρους πρέπει να παρακολουθούνται και να ενημερώνονται με νέες εκδόσεις service pack και patches.

Οι σημαντικές αναβαθμίσεις του συστήματος πρέπει να δοκιμαστούν διεξοδικά παράλληλα με το υπάρχον σύστημα σε ένα ασφαλές περιβάλλον δοκιμών που αντιγράφει το λειτουργικό σύστημα.

Όλες οι σημαντικές αλλαγές στην κύρια υποδομή (πχ. Δίκτυο, υπολογιστές) πρέπει να αξιολογούνται για τον αντίκτυπό τους στην ασφάλεια των πληροφοριών ως μέρος της τυποποιημένης εκτίμησης κινδύνου.

2.3.2 Προστασία από κακόβουλο λογισμικό

Λαμβάνονται τα κατάλληλα μέτρα για την προστασία όλων των πληροφοριακών συστημάτων του «Δήμου Κιλκίς», της υποδομής και των πληροφοριών από το κακόβουλο λογισμικό.

Ένα αποτελεσματικό και πάντα ενημερωμένο με τις τελευταίες εκδόσεις λογισμικό προστασίας από ιούς εκτελείται σε όλους τους διακομιστές και τους υπολογιστές.

Προκειμένου να αποφευχθεί το κακόβουλο λογισμικό, θα δημιουργηθούν κατάλληλοι έλεγχοι πρόσβασης (πχ. δικαιώματα διαχειριστή / χρήστη) για να αποφευχθεί η εγκατάσταση λογισμικού από όλους τους χρήστες.

Το κακόβουλο λογισμικό κινητής τηλεφωνίας αντιπροσωπεύει νεότερες τεχνολογίες που βρίσκονται συχνά σε ιστοσελίδες και ηλεκτρονικά ταχυδρομεία και περιλαμβάνει, αλλά δεν περιορίζεται σε:

- ActiveX
- Java
- JavaScript
- VBScript
- Macros
- HTTPS
- HTML

Το προσωπικό του «Δήμου Κιλκίς», είναι υπεύθυνο να διασφαλίσει ότι δεν εισάγει κακόβουλο λογισμικό στα συστήματα πληροφορικής του «Δήμου Κιλκίς».

Σε περίπτωση ανίχνευσης ενός ιού σε ένα σύστημα του «Δήμου Κιλκίς», ο χρήστης πρέπει να ενημερώσει τον Διαχειριστή Ασφάλειας Πληροφοριών.

Όλοι οι διακομιστές πρέπει να έχουν εφαρμόσει τις κατάλληλες κρίσιμες ενημερωμένες εκδόσεις ασφαλείας μόλις καταστούν διαθέσιμες και έχουν περάσει τη δοκιμή αποδοχής του συστήματος. Όλα τα άλλα patches πρέπει να εφαρμόζονται ανάλογα με την περίπτωση.

Πρέπει να υπάρχει πλήρης καταγραφή των επιδιορθώσεων που έχουν εφαρμοστεί και πότε.

Οι αιτήσεις εγκατάστασης λογισμικού γίνονται αποδεκτές μόνον εφόσον υπάρχει σαφής τεχνική επαλήθευση.

2.3.3 Δημιουργία αντιγράφων ασφαλείας

Πρέπει να λαμβάνονται τακτικά αντίγραφα σημαντικών υπηρεσιακών πληροφοριών για να διασφαλιστεί ότι ο οργανισμός μπορεί να ανακάμψει από καταστροφή, απόσπαση μέσων ή σφάλμα.

Ένας κατάλληλος κύκλος backup πρέπει να χρησιμοποιηθεί και να τεκμηριωθεί πλήρως.

Τυχόν τρίτα μέρη που αποθηκεύουν πληροφορίες οργανισμού πρέπει επίσης να υποχρεούνται να διασφαλίζουν ότι στις πληροφορίες δημιουργούνται αντίγραφα ασφαλείας.

Αποθηκεύστε και ένα πλήρες κρυπτογραφημένο αντίγραφο ασφαλείας μαζί με τη διαδικασία ανάκτησης, σε μια εξωτερική τοποθεσία εκτός από το αντίγραφο στο κεντρικό κτήριο.

Βεβαιωθείτε ότι η απομακρυσμένη τοποθεσία είναι επαρκώς απομακρυσμένη για να αποφύγετε να επηρεαστεί από οποιαδήποτε καταστροφή που συμβαίνει στον κύριο χώρο.

Η πλήρης τεκμηρίωση της διαδικασίας ανάκτησης πρέπει να δημιουργηθεί και να αποθηκευτεί.

Εκτελέστε τακτικές αποκαταστάσεις πληροφοριών από αντίγραφα ασφαλείας για να διασφαλίσετε την αξιοπιστία των μέσων δημιουργίας αντιγράφων ασφαλείας και τη διαδικασία επαναφοράς.

2.3.4 Χειρισμός μέσων αποθήκευσης

Τα μέσα αποθήκευσης περιλαμβάνουν, αλλά δεν περιορίζονται, τα ακόλουθα:

- Σκληροί δίσκοι υπολογιστών (εσωτερικοί και εξωτερικοί)
- CD
- DVD
- Οπτικοί δίσκοι
- Μνήμες Memory Stick USB
- Αναγνώστες καρτών μέσων
- Συσκευές αναπαραγωγής MP3
- Ταινίες δημιουργίας αντιγράφων ασφαλείας

- Ταινίες ήχου (συμπεριλαμβανομένων των συσκευών εγγραφής και των μηχανημάτων απάντησης)
- Χαρτί

Τα αφαιρούμενα μέσα ηλεκτρονικών υπολογιστών (πχ. κασέτες, δίσκοι και εκτυπωμένες αναφορές) πρέπει να προστατεύονται για να αποφευχθεί ζημιά, κλοπή ή μη εξουσιοδοτημένη πρόσβαση.

Τα μέσα αποθήκευσης που μεταφέρονται πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση ή καταστροφή.

Πρέπει να τεθούν οι κατάλληλες ρυθμίσεις για να εξασφαλιστεί η μελλοντική διαθεσιμότητα δεδομένων που απαιτείται πέρα από τη διάρκεια ζωής των μέσων δημιουργίας αντιγράφων ασφαλείας ή άλλων αποθηκευτικών μεθόδων:

- Η επιλογή μακροπρόθεσμων μέσων αποθήκευσης πρέπει να λαμβάνει υπόψη τα φυσικά χαρακτηριστικά του μέσου και το χρονικό διάστημα που θα χρησιμοποιηθεί.
- Όταν οι εγγραφές πρέπει να αποθηκεύονται νομικά (ή πρακτικά) σε χαρτί, πρέπει να λαμβάνονται επαρκείς προφυλάξεις ώστε να εξασφαλίζεται ότι οι περιβαλλοντικές συνθήκες παραμένουν κατάλληλες για τον τύπο του χρησιμοποιούμενου χαρτιού. Όπου είναι δυνατόν, πρέπει να λαμβάνονται αντίγραφα ασφαλείας τέτοιων δεδομένων με μεθόδους όπως η σάρωση ή η φωτογράφηση. Πρέπει να γίνονται τακτικοί έλεγχοι για να εκτιμηθεί ο βαθμός αλλοίωσης του χαρτιού και τα μέτρα που πρέπει να ληφθούν για τη διατήρηση των δεδομένων, εφόσον απαιτείται.
- Για δεδομένα που είναι αποθηκευμένα σε ηλεκτρονικά μέσα, όπως σκληροί δίσκοι, CD, DVD, USB memory, ταινία, πρέπει να ληφθούν παρόμοια μέτρα για να διασφαλιστεί η μακροζωία των υλικών, συμπεριλαμβανομένης της σωστής αποθήκευσης και αντιγραφής σε πιο εύρωστα μέσα, εάν είναι απαραίτητο. Η ικανότητα ανάγνωσης του περιεχομένου της συγκεκριμένης μορφής CD, DVD, ταινίας (ή άλλης ανάλογης μορφής) πρέπει να διατηρείται διατηρώντας μια συσκευή ικανή να την επεξεργαστεί. Εάν αυτό δεν είναι πρακτικό, μπορεί να χρησιμοποιηθεί εξωτερικό τρίτο μέρος για τη μετατροπή των μέσων σε μια εναλλακτική μορφή.

Τα μέσα αποθήκευσης που περιέχουν δεδομένα που έφτασαν στο τέλος της ζωής τους, σύμφωνα με την καθορισμένη πολιτική,δεν χρειάζονται πλέον διαγράφονται ή καταστρέφονται με ασφάλεια για να αποφευχθεί η διαρροή δεδομένων. Η διαδικασία καταστροφής θα πρέπει να καταγράφεται με πλήρη αιτιολόγηση για τα προσωπικά δεδομένα, και η καταγραφή αυτή πρέπει να διατηρείται ως αποδεικτικό στοιχείο.

2.3.5 Αρχεία και πληροφορίες καταγραφής

Τα αρχεία καταγραφής θα πρέπει να ενεργοποιούνται για κάθε σύστημα / εφαρμογή που χρησιμοποιείται για την επεξεργασία των προσωπικών δεδομένων. Πρέπει να περιλαμβάνουν όλους τους τύπους πρόσβασης στα δεδομένα (προβολή, τροποποίηση, διαγραφή).

Στα κρίσιμα συστήματα τα αρχεία καταγραφής ελάχιστων ελέγχων πρέπει να περιέχουν τουλάχιστον τις ακόλουθες πληροφορίες:

- Ταυτότητα συστήματος πρόσβασης (υπολογιστής, πρόγραμμα λογισμικού, κλπ.)
- Ταυτότητα χρήστη
- Ημερομηνία και ώρα
- Επιτυχής / μη επιτυχής σύνδεση
- Επιτυχής / μη επιτυχής αποσύνδεση
- Μη εξουσιοδοτημένη πρόσβαση σε εφαρμογές
- Αλλαγές στις διαμορφώσεις του συστήματος
- Χρήση προνομιούχων λογαριασμών (πχ. διαχείριση λογαριασμού, αλλαγές πολιτικής, διαμόρφωση συσκευών)
- Εκτύπωση αρχείων με προσωπικά δεδομένα

Προστατεύεται η πρόσβαση στα αρχεία καταγραφής από μη εξουσιοδοτημένη πρόσβαση, η οποία θα μπορούσε να έχει ως αποτέλεσμα την αλλοίωση ή τη διαγραφή εγγραφών.

Δεν θα πρέπει να υφίσταται δυνατότητα διαγραφής των αρχείων καταγραφής του συστήματος από ένα μόνο άτομο. Τέτοια διαγραφή θα πρέπει να γίνεται με την παρουσία 2 τουλάχιστον ατόμων, τα οποία θα έχουν διαφορετικούς ρόλους (πχ. Διαχειριστής Ασφαλείας + διοικητικός διευθυντής).

Το υπηρεσιακό προσωπικό και οι διαχειριστές συστημάτων πρέπει να τηρούν αρχείο των δραστηριοτήτων τους. Τα ημερολόγια πρέπει να περιλαμβάνουν:

- Χρόνοι αντιγράφων ασφαλείας και λεπτομέρειες ανταλλαγής εφεδρικών ταινιών
- Ο χρόνος έναρξης και λήξης συμβάντος συστήματος και ο εμπλεκόμενος
- Σφάλματα συστήματος (τι, ημερομηνία, ώρα) και διορθωτικές ενέργειες

Τα αρχεία καταγραφής πρέπει να ελέγχονται τακτικά για να εξασφαλίζεται η τήρηση των σωστών διαδικασιών.

Όλα τα ρολόγια υπολογιστή πρέπει να συγχρονίζονται με μια σταθερή πηγή ώρας (http://time.eim.gr) για να διασφαλιστεί η ακρίβεια όλων των αρχείων καταγραφής ελέγχου συστημάτων, καθώς μπορεί να χρειαστούν για την έρευνα περιστατικών.

Πρέπει να καταγράφονται οι ενέργειες των διαχειριστών συστημάτων και των χειριστών συστημάτων, συμπεριλαμβανομένης της προσθήκης / διαγραφής / αλλαγής δικαιωμάτων χρήστη.

Οι παραβιάσεις προσωπικών δεδομένων πρέπει να καταγράφονται στο αρχείο ***GDPR-DOC-19 Μητρώο Παραβιάσεων Προσωπικών Δεδομένων*** για την υποστήριξη της λογοδοσίας στην Αρχή Προστασίας Δεδομένων.

Ελλείψει άλλων μηχανισμών, η επεξεργασία προσωπικών δεδομένων θα πρέπει να καταγράφεται στο αρχείο ***GDPR-FORM-12 Φόρμα Ανάλυσης Προσωπικών Δεδομένων***

2.3.6 Διαχείριση Δικτύου

Η διαχείριση δικτύου είναι κρίσιμη για την παροχή υπηρεσιών οργάνωσης.

Οι συνδέσεις με την υποδομή δικτύου του «Δήμου Κιλκίς», πραγματοποιούνται με ελεγχόμενο τρόπο.

Τα ασύρματα δίκτυα πρέπει να αποφεύγονται σαν μέρος ή επέκταση του υπηρεσιακού δικτύου του «Δήμου Κιλκίς».

Πρέπει να υπάρχει καταγραφή όλων των στοιχείων του δικτύου σε ένα μητρώο στοιχείων.

Όλοι οι κεντρικοί υπολογιστές έχουν ενισχυμένη την ασφάλεια σε κατάλληλο επίπεδο.

Όλες οι υπηρεσίες δικτύου των λειτουργικών συστημάτων που δεν χρειάζονται πρέπει να απενεργοποιηθούν.

Πρέπει να υπάρχει τουλάχιστον τείχος προστασίας(firewall) για τον επαρκή έλεγχο των δικτυακών συνδέσεων του εσωτερικού δικτύου του υπευθύνου επεξεργασίας από και προς το διαδίκτυο ή άλλα εξωτερικά μη έμπιστα δίκτυα.

Οι συνδέσεις που ενεργοποιούνται μέσω του firewall και οι υπηρεσίες που εξυπηρετούν πρέπει να εγκρίνονται από τον Διαχειριστή Ασφάλειας. Πρέπει, επίσης, να τηρείται επικαιροποιημένος κατάλογος με τις εγκεκριμένες συνδέσεις από και προς το δίκτυο του υπευθύνου επεξεργασίας και τις υπηρεσίες που εξυπηρετούν.

2.3.7 Χρήση της Κρυπτογράφησης

Χρησιμοποιούνται μόνο διεθνείς και αναγνωρισμένοι μηχανισμοί κρυπτογράφησης.

Η κρυπτογράφηση υλοποιείται μόνο μέσω του εξουσιοδοτημένου λογισμικού της υπηρεσίας.

Ο διαχειριστής ασφαλείας καταγράφει το εξουσιοδοτημένο λογισμικό, τις υπηρεσίες καθώς και τις παραμέτρους για την κρυπτογράφηση.

Οι μηχανισμοί κρυπτογράφησης καθώς και οι απαιτήσεις του μήκους κλειδιού αναθεωρούνται ετησίως και αναβαθμίζονται ως εκεί που η τεχνολογία το επιτρέπει.

Δεν θα πρέπει να χρησιμοποιούνται οι αλγόριθμοι και τα πρωτόκολλα DES, MD5, RC4, SSL τα οποία αποδεδειγμένα έχουν κενά ασφαλείας.

Η κρυπτογράφηση της επικοινωνίας θα πρέπει να επιτυγχάνεται μέσω του πρωτοκόλλου TLS v1.2 ή IPSec.

Να χρησιμοποιηθούν εγκεκριμένες, από διεθνείς οργανισμούς πιστοποίησης, τεχνικές/πρακτικές TLS/IPSec Tunneling.

Σε περίπτωση που ανακαλυφθεί κάποια αδυναμία στους κρυπτογραφικούς αλγορίθμους, που χρησιμοποιούνται, όπως αυτή προκύψει από ανακοινώσεις γνωστών οργανισμών πιστοποίησης ή αναγνωρισμένων επιστημονικών περιοδικών και διεθνών επιστημονικών συνεδρίων, θα πρέπει να απαγορευτεί η χρήση τους και να αντικατασταθούν από άλλους υψηλότερης ασφάλειας.

Εάν υπάρχει ανάγκη για την χρήση ασύρματων δικτύων τότε θα πρέπει να χρησιμοποιηθεί το πρωτόκολλο WPA2 με χρήση ψηφιακών πιστοποιητικών.

Η υλοποίηση των απαραίτητων μηχανισμών κρυπτογράφησης θα είναι συμμορφώνεται με την παρούσα πολιτική

Όπου ενδείκνυται πρέπει να χρησιμοποιούνται τεχνικές κρυπτογράφησης και ψευδοανωνυμοποίησης για την εξασφάλιση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων.

Πρέπει να ληφθεί μέριμνα ώστε τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων να αποθηκεύονται με ασφάλεια για τη ζωή των σχετικών δεδομένων και να συμμορφώνονται με την πολιτική του οργανισμού για την κρυπτογράφηση.

2.3.8 Διαχείριση αλλαγών

Οι αλλαγές στα συστήματα που επεξεργάζονται προσωπικά δεδομένα θα πρέπει να ελέγχονται, καθώς αποτελούν αρκετά συχνά αιτία προβλημάτων.

Θα πρέπει να τεκμηριωθούν οι επίσημες διαδικασίες έγκρισης των προτεινόμενων αλλαγών και καθήκοντα, μέσω των οποίων να ελέγχονται όλες οι αλλαγές σε εξοπλισμό, λογισμικό και διαδικασίες επεξεργασίας προσωπικών δεδομένων.

Όλες οι αλλαγές θα πρέπει να εγκρίνονται πριν υλοποιηθούν:

- Οι αιτήσεις των αλλαγών θα πρέπει να εγκρίνονται από τον υπεύθυνο Πληροφορικής.
- Οι αιτήσεις που επηρεάζουν τους μηχανισμούς ασφαλείας θα πρέπει να εγκρίνονται από τον υπεύθυνο ασφάλειας.
- Οι αιτήσεις που επηρεάζουν την επεξεργασία των προσωπικών δεδομένων θα πρέπει να εγκρίνονται από τον προστασίας δεδομένων.

Θα πρέπει να τηρείται αρχείο μεταβολών με τις αλλαγές.

Οι τροποποιήσεις να πραγματοποιούνται σε σύστημα ελέγχου και να δοκιμάζονται πριν τεθούν σε παραγωγική λειτουργία.

Θα πρέπει να ελέγχονται οι πιθανές συνέπειες των αλλαγών κυρίως σε θέματα ασφάλειας και επεξεργασίας προσωπικών δεδομένων.

Θα πρέπει να κοινοποιούνται όλες οι σχετικές λεπτομέρειες για κάθε αλλαγή στα αρμόδια στελέχη του Δήμου. Να περιλαμβάνονται τα ακόλουθα στοιχεία:

- Κωδικός αλλαγής
- Περιγραφή τις αλλαγής – αιτιολογία της αλλαγής
- Εισηγητής της αλλαγής
- Ρόλοι και Αρμοδιότητες που εμπλέκονται
- Κριτήρια αποδοχής της αλλαγής
- Πιθανές επιπτώσεις
- Προετοιμασία της αλλαγής
- Χρονοδιάγραμμα δράσεων
- Διαδικασία υλοποίησης της αλλαγής
- Διαδικασία επαναφοράς του συστήματος σε περίπτωση ανεπιτυχούς αλλαγής

- Πλάνο ελέγχων ορθής λειτουργίας μετά την αλλαγή

2.3.9 Ετήσιος διαγνωστικός έλεγχος

Ένας ετήσιος έλεγχος υγείας όλων των συστημάτων και εγκαταστάσεων υποδομής πληροφορικής καθώς και της διατήρησης και της αποθήκευσης των δεδομένων , πρέπει να διενεργείται από τον εσωτερικό έλεγχο κάθε 12 μήνες.

Αυτός ο έλεγχος υγείας πρέπει να περιλαμβάνει, μεταξύ άλλων, τα ακόλουθα:

- Πλήρης δοκιμή διείσδυσης
- Σάρωση δικτύου που θα εντοπίσει όλες τις συσκευές με διευθύνσεις IP
- Ανάλυση ευπάθειας, συμπεριλαμβανομένων των επιπέδων των επιδιορθώσεων, των κακών κωδικών πρόσβασης και των υπηρεσιών που χρησιμοποιούνται
- Συνοπτική έκθεση με συστάσεις για βελτίωση

Η επιθεώρηση της διατήρησης και η αποθήκευσης των δεδομένων πρέπει να εκτελείται ώστε να εξασφαλίζεται ότι:

- Η πολιτική διατήρησης και προστασίας δεδομένων παραμένει έγκυρη
- Τα δεδομένα διατηρούνται σύμφωνα με την πολιτική
- Τα δεδομένα διαγράφονται με ασφάλεια όταν πλέον δεν χρειάζονται
- Πληρούνται οι νομικές, ρυθμιστικές και συμβατικές υποχρεώσεις
- Οι διαδικασίες για την επιθεώρηση δεδομένων ικανοποιούν τις υπηρεσιακές απαιτήσεις

Τα αποτελέσματα αυτών των ελέγχων πρέπει να καταγράφονται

2.4 Υποδομές φύλαξης δεδομένων

2.4.1 Ασφαλείς περιοχές

Τα δεδομένα πρέπει να αποθηκεύονται με ασφάλεια.

Η εκτίμηση επικινδυνότητας πρέπει να προσδιορίζει το κατάλληλο επίπεδο προστασίας που πρέπει να εφαρμόζεται για τη διασφάλιση της αποθήκευσης των δεδομένων.

Η φυσική ασφάλεια πρέπει να αρχίζει με το ίδιο το κτίριο και πρέπει να διεξάγεται αξιολόγηση της ευαισθησίας της περιμέτρου.

Το κτίριο πρέπει να διαθέτει τους κατάλληλους μηχανισμούς ελέγχου για τον τύπο δεδομένων και εξοπλισμού που αποθηκεύονται εκεί. Αυτά θα μπορούσαν να περιλαμβάνουν, αλλά δεν περιορίζονται στα εξής:

- Οι συναγερμοί τοποθετούνται και ενεργοποιούνται εκτός ωρών εργασίας

- Κλειδαριές παραθύρων και θυρών
- Ρολά παραθύρων στους χαμηλότερους ορόφους
- Μηχανισμοί ελέγχου πρόσβασης που είναι εγκατεστημένοι σε όλες τις προσβάσιμες πόρτες (όπου χρησιμοποιούνται κωδικοί, θα πρέπει να αλλάζουν τακτικά και να είναι γνωστοί μόνο σε όσους έχουν άδεια πρόσβασης στην περιοχή / κτίριο)
- Κάμερες CCTV
- Προστασία από βλάβες - πχ. πυρκαγιά, πλημμύρα, βανδαλισμό

Το προσωπικό που εργάζεται σε ασφαλείς περιοχές θα πρέπει να αμφισβητήσει όποιον δεν φέρει σήμα ή αντιλαμβάνεται ότι δεν ανήκει στο εξουσιοδοτημένο προσωπικό.

Τα αναγνωριστικά και τα εργαλεία πρόσβασης / διέλευσης (πχ. διακριτικά, κλειδιά, κωδικοί εισόδου κλπ.) πρέπει να τηρούνται μόνο από υπαλλήλους που έχουν εξουσιοδοτηθεί να έχουν πρόσβαση σε αυτές τις περιοχές και δεν πρέπει να δανείζονται / παρέχονται σε κανέναν άλλο.

Τα κλειδιά σε όλες τις ασφαλείς περιοχές που στεγάζουν τον εξοπλισμό πληροφορικής και τα ντουλάπια IT που κλειδώνουν, αποθηκεύονται κεντρικά από τον Διαχειριστή Ασφάλειας Πληροφοριών ανάλογα με την περίπτωση.

Σε όλες τις περιπτώσεις όπου υπάρχουν διαδικασίες ασφαλείας, πρέπει να εκδοθούν οδηγίες για την αντιμετώπιση της παράβασης ασφαλείας.

Σε περίπτωση που υπάρχουν παραβιάσεις ή όταν ένα μέλος του προσωπικού αποχωρεί εκτός των κανονικών συνθηκών τερματισμού, όλα τα εργαλεία αναγνώρισης / πρόσβασης (πχ. εμβλήματα, κλειδιά κλπ.) θα πρέπει να ανακτηθούν από το μέλος του προσωπικού και οι κωδικοί θυρών / πρόσβασης θα πρέπει να αλλάξουν αμέσως.

2.4.2 Ασφάλεια χαρτιού και εξοπλισμού

Για τα δεδομένα που αποτυπώνονται σε χαρτί (ή σε παρόμοιες μη ηλεκτρονικές πληροφορίες) πρέπει να ανατεθεί ένας κάτοχος να ακολουθούνται οι έλεγχοι ασφαλείας των δεδομένων για την προστασία τους.

Το χαρτί σε ένα ανοικτό γραφείο πρέπει να προστατεύεται μέσω κατάλληλων μέτρων που θα μπορούσαν να περιλαμβάνουν, αλλά δεν περιορίζονται στα εξής:

- Ντουλάπια αρχειοθέτησης που κλειδώνονται με τα κλειδιά που είναι αποθηκευμένα μακριά από το ντουλάπι
- Χρηματοκιβώτια κλειδωμένα

- Αποθηκευμένο σε ασφαλή περιοχή που προστατεύεται από μη εξουσιοδοτημένη πρόσβαση
- Μετά το πέρας των εργασιών τα έγγραφα καθώς και τα CD, DVD και τα USB sticks με προσωπικά δεδομένα πρέπει να κλειδώνονται σε ντουλάπες ή συρτάρια (πολιτική καθαρού γραφείου)

Όλος ο γενικός εξοπλισμός πληροφορικής πρέπει να βρίσκεται σε κατάλληλες φυσικές τοποθεσίες που:

- Περιορίζουν τους κινδύνους από περιβαλλοντικούς κινδύνους - πχ. θερμότητα, πυρκαγιά, καπνό, νερό, σκόνη και δονήσεις
- Περιορίζουν τον κίνδυνο κλοπής - πχ. **αν χρειάζεται**, τα στοιχεία όπως οι φορητοί υπολογιστές θα πρέπει να συνδέονται φυσικά με το γραφείο
- Οι σταθμοί εργασίας που χειρίζονται ευαίσθητα δεδομένα θα πρέπει να λειτουργούν με τρόπο ώστε να αποφεύγεται ο κίνδυνος να φαίνονται τα δεδομένα σε μη εξουσιοδοτημένα άτομα

Τα δεδομένα πρέπει να αποθηκεύονται στους διακομιστές αρχείων δικτύου όπου χρειάζεται. Αυτό εξασφαλίζει ότι οι πληροφορίες που έχουν χαθεί, κλαπεί ή καταστραφεί μέσω μη εξουσιοδοτημένης πρόσβασης μπορούν να αποκατασταθούν με την ακεραιότητά τους να διατηρείται.

Όλοι οι servers που βρίσκονται εκτός του κέντρου δεδομένων πρέπει να βρίσκονται σε φυσικά ασφαλές περιβάλλον.

Τα κρίσιμα για την υπηρεσία συστήματα πρέπει να προστατεύονται από ένα μη διακοπτόμενο τροφοδοτικό (UPS), προκειμένου να μειωθεί το λειτουργικό σύστημα και ο κίνδυνος διαφθοράς δεδομένων από αποτυχίες ρεύματος.

Όλα τα είδη εξοπλισμού πρέπει να καταγράφονται σε κατάλογο

Πρέπει να υπάρχουν διαδικασίες για την ενημέρωση των αποθεμάτων μόλις ληφθούν ή διατεθούν τα περιουσιακά στοιχεία.

Όλος ο εξοπλισμός πρέπει να φέρει ασφάλεια και να έχει έναν μοναδικό αριθμό ενεργητικού που του έχει χορηγηθεί. Αυτός ο αριθμός του ενεργητικού θα πρέπει να καταγράφεται στο απόθεμα IT.

Τα καλώδια που μεταφέρουν δεδομένα ή υποστηρίζουν βασικές υπηρεσίες πληροφοριών πρέπει να προστατεύονται από την υποκλοπή ή τη ζημία.

Τα καλώδια τροφοδοσίας θα πρέπει να διαχωρίζονται από τα καλώδια δικτύου για να αποφεύγονται παρεμβολές

Τα καλώδια δικτύου πρέπει να προστατεύονται με αγωγούς και όπου είναι δυνατόν να αποφεύγονται διαδρομές μέσω δημόσιων χώρων.

2.4.3 Διαχείριση του κύκλου ζωής του εξοπλισμού

Ο Διαχειριστής Ασφάλειας Πληροφοριών και οι τρίτοι προμηθευτές πρέπει να διασφαλίσουν ότι όλος ο εξοπλισμός (πληροφορικής και διαγνωστικών μηχανημάτων) του «Δήμου Κιλκίς», συντηρείται σύμφωνα με τις οδηγίες του κατασκευαστή και με τυχόν τεκμηριωμένες εσωτερικές διαδικασίες για να διασφαλιστεί ότι παραμένει σε κατάσταση λειτουργίας.

Το προσωπικό που ασχολείται με τη συντήρηση πρέπει να:

- Διατηρεί όλα τα αντίγραφα των οδηγιών του κατασκευαστή
- Γνωρίζει τα συνιστώμενα διαστήματα και προδιαγραφές συντήρησης
- Βεβαιώνεται ότι μόνο οι εξουσιοδοτημένοι τεχνικοί ολοκληρώνουν οποιαδήποτε εργασία στον εξοπλισμό
- Καταγράφει τις λεπτομέρειες όλων των διορθωτικών εργασιών που πραγματοποιήθηκαν
- Προσδιορίζει τυχόν ασφαλιστικές απαιτήσεις
- Καταγράφει τις λεπτομέρειες των ελαττωμάτων και των απαιτούμενων ενεργειών

Πρέπει να τηρείται αρχείο ιστορικού σέρβις του εξοπλισμού ώστε, όταν ο εξοπλισμός να γίνει παλαιότερος, να ληφθούν αποφάσεις σχετικά με τον κατάλληλο χρόνο για την αντικατάστασή του.

Η συντήρηση του εξοπλισμού πρέπει να είναι σύμφωνη με τις οδηγίες του κατασκευαστή. Αυτό πρέπει να είναι τεκμηριωμένο και διαθέσιμο για να χρησιμοποιήσει το προσωπικό υποστήριξης κατά την οργάνωση των επισκευών.

Η χρήση του εξοπλισμού εκτός του χώρου πρέπει να εγκριθεί επίσημα από τον διευθυντή του χρήστη.

Ο εξοπλισμός που πρόκειται να επαναχρησιμοποιηθεί ή να απορριφθεί πρέπει να έχει σβήσει / καταστρέψει με ασφάλεια όλα τα δεδομένα και το λογισμικό του.

Προκειμένου να επιβεβαιωθεί η ακρίβεια και η κατάσταση των παραδόσεων και να αποφευχθεί η απώλεια ή κλοπή αποθηκευμένου εξοπλισμού, πρέπει να εφαρμοστούν τα εξής:

- Οι παραδόσεις εξοπλισμού πρέπει να υπογράφονται από εξουσιοδοτημένο άτομο χρησιμοποιώντας μια ελεγχόμενη τυπική διαδικασία. Αυτή η διαδικασία θα πρέπει να επιβεβαιώσει ότι τα παραδοθέντα αντικείμενα αντιστοιχούν πλήρως στον κατάλογο του δελτίου παράδοσης. Τα πραγματικά περιουσιακά στοιχεία που ελήφθησαν πρέπει να καταγράφονται
- Οι χώροι φόρτωσης και οι χώροι αποθήκευσης πρέπει να είναι επαρκώς ασφαλισμένοι έναντι μη εξουσιοδοτημένης πρόσβασης και κάθε πρόσβαση πρέπει να είναι ελεγχόμενη

- Η μεταγενέστερη κατάργηση του εξοπλισμού πρέπει να γίνεται μέσω επίσημης, ελεγχόμενης διαδικασίας

Πρέπει να υπάρχει υποχρέωση ελέγχου των ρυθμίσεων για την ασφάλεια των πληροφοριών σε τακτική βάση ώστε να παρέχεται ανεξάρτητη εκτίμηση και να προτείνονται βελτιώσεις ασφαλείας, όπου χρειάζεται.

2.5 Πρόσβαση σε Πληροφορικά συστήματα

2.5.1 Γενικά

Όλοι οι κωδικοί πρόσβασης σε επίπεδο χρήστη πρέπει να αλλάζονται τουλάχιστον μια φορά στους 6 μήνες ή κάθε φορά που ένα σύστημα προτρέπει τον χρήστη να το αλλάξει.

Το ελάχιστο μήκος κωδικού πρόσβασης για την αξιολόγηση διαμόρφωσης είναι 8 χαρακτήρες

Οι κωδικοί πρόσβασης πρέπει να πληρούν τις απαιτήσεις πολυπλοκότητας περιλαμβάνοντας τουλάχιστον ένα κεφαλαίο γράμμα, έναν αριθμό και ένα Μη αλφαριθμητικό χαρακτήρα.

Οι χρήστες **δεν πρέπει** να επαναχρησιμοποιούν τον ίδιο κωδικό πρόσβασης με τις προηγούμενες 10 αλλαγές κωδικού πρόσβασης.

Όλα τα συστήματα και οι διαδικασίες του «Δήμου Κιλκίς», θα εφαρμοστούν για την επιβολή των ακόλουθων:

- Έλεγχος ταυτότητας μεμονωμένων χρηστών, όχι ομάδων χρηστών - δηλ. Δεν υπάρχουν γενικοί λογαριασμοί
- Προστασία όσον αφορά την ανάκτηση κωδικών πρόσβασης και στοιχείων ασφαλείας
- Παρακολούθηση και καταγραφή πρόσβασης στο σύστημα - σε επίπεδο χρήστη
- Διαχείριση ρόλων έτσι ώστε να μπορούν να εκτελούνται λειτουργίες χωρίς να μοιράζονται κωδικούς πρόσβασης
- Οι διαδικασίες διαχείρισης κωδικού πρόσβασης πρέπει να ελέγχονται σωστά, και να είναι ασφαλείς
- Τα αναγνωριστικά χρηστών (όνομα και κωδικός) είναι μοναδικά, δεν μοιράζονται ή κοινοποιούνται σε κανένα άλλο χρήστη

Οι τυπικές διαδικασίες ελέγχου πρόσβασης των χρηστών πρέπει να τεκμηριώνονται, να εφαρμόζονται και να ενημερώνονται για κάθε σύστημα εφαρμογής και πληροφοριών, ώστε να εξασφαλίζεται η εξουσιοδοτημένη πρόσβαση των χρηστών και να προλαμβάνεται η μη εξουσιοδοτημένη πρόσβαση.

Πρέπει να καλύπτουν όλα τα στάδια του κύκλου ζωής της πρόσβασης των χρηστών, από την αρχική εγγραφή νέων χρηστών στην τελική κατάργηση της εγγραφής των χρηστών που δεν χρειάζονται πλέον πρόσβαση.

Τα δικαιώματα πρόσβασης των χρηστών πρέπει να επανεξετάζονται σε τακτά χρονικά διαστήματα ώστε να εξασφαλίζεται ότι εξακολουθούν να χορηγούνται τα κατάλληλα δικαιώματα.

Οι λογαριασμοί διαχείρισης συστήματος πρέπει να παρέχονται μόνο σε χρήστες που είναι υποχρεωμένοι να εκτελούν εργασίες διαχείρισης του συστήματος.

Όταν ένας εργαζόμενος εγκαταλείπει την υπηρεσία, η πρόσβασή του σε συστήματα πληροφορικής και δεδομένα πρέπει να αναστέλλεται κατά το κλείσιμο της υπηρεσίας την τελευταία εργάσιμη ημέρα του εργαζομένου. Είναι ευθύνη του υπεύθυνου προσωπικού να ζητήσει την αναστολή των δικαιωμάτων πρόσβασης μέσω του γραφείου υπηρεσιών πληροφορικής.

2.5.2 Έλεγχος πρόσβασης διακομιστή και εφαρμογών

Η πρόσβαση στους διακομιστές ελέγχεται από μια ασφαλή διαδικασία σύνδεσης.

Η διαδικασία σύνδεσης πρέπει επίσης να προστατεύεται με:

- Να μην εμφανίζονται προηγούμενες πληροφορίες σύνδεσης, πχ. όνομα χρήστη
- Περιορισμός του αριθμού των ανεπιτυχών προσπαθειών και κλειδώματος του λογαριασμού σε περίπτωση υπέρβασης
- Οι χαρακτήρες κωδικού πρόσβασης να είναι κρυμμένοι με σύμβολα
- Με την εμφάνιση γενικής προειδοποίησης ότι επιτρέπονται μόνο εξουσιοδοτημένοι χρήστες

Οι διαχειριστές συστήματος πρέπει να έχουν μεμονωμένους λογαριασμούς διαχειριστή που θα καταγράφονται και θα ελέγχονται.

Η πρόσβαση σε εφαρμογές λογισμικού πρέπει να περιοριστεί χρησιμοποιώντας τα χαρακτηριστικά ασφαλείας που είναι ενσωματωμένα στο συγκεκριμένο προϊόν.

Ο «ιδιοκτήτης» της εφαρμογής λογισμικού είναι υπεύθυνος για τη χορήγηση πρόσβασης στις πληροφορίες εντός του συστήματος.

Η πρόσβαση πρέπει:

- Να συμμορφώνεται με την προηγούμενη ενότητα «Γενικά»
- Να δίνεται το κατάλληλο επίπεδο πρόσβασης που απαιτείται για το ρόλο του χρήστη
- Να μην είναι δυνατή η αντικατάσταση (με αφαίρεση ή απόκρυψη των ρυθμίσεων διαχείρισης από το χρήστη)
- Να μπορούν να τροποποιηθούν τα δικαιώματα που έχουν κληρονομηθεί από το λειτουργικό σύστημα που θα μπορούσαν να επιτρέψουν μη εξουσιοδοτημένα υψηλότερα επίπεδα πρόσβασης
- Να καταγράφεται και να ελέγχεται

2.5.3 Απομακρυσμένη πρόσβαση από Προμηθευτή

Η απομακρυσμένη πρόσβαση στα συστήματα του «Δήμου Κιλκίς» από τους προμηθευτές πρέπει να ελέγχεται αυστηρά.

Οποιεσδήποτε αλλαγές στις συνδέσεις του προμηθευτή πρέπει να αποσταλούν αμέσως στον Διαχειριστή Ασφάλειας Πληροφοριών για να ενημερωθεί ή να σταματήσει η πρόσβαση.

Οι Συνεργάτες ή οι προμηθευτές πρέπει να ορίσουν τα εξουσιοδοτημένα άτομα που θα έχουν πρόσβαση στα συστήματα και να ενημερώσουν το «Δήμο Κιλκίς». Οποιαδήποτε αλλαγή στα άτομα πρέπει να κοινοποιείται επίσημα και έγκαιρα.

Οι Συνεργάτες ή οι προμηθευτές πρέπει να επικοινωνήσουν με τον Διαχειριστή Ασφάλειας Πληροφοριών πριν συνδεθούν στο δίκτυο του «Δήμου Κιλκίς», και πρέπει να τηρηθούν τα αρχεία δραστηριότητας.

Οι Συνεργάτες ή οι προμηθευτές πρέπει να ενημερώσουν τον Διαχειριστή Ασφάλειας Πληροφοριών όταν ολοκληρωθεί η επικοινωνία.

Το λογισμικό απομακρυσμένης πρόσβασης πρέπει να απενεργοποιείται όταν δεν χρησιμοποιείται.

Η επικοινωνία πρέπει να γίνεται μέσω ασφαλών καναλιών (πχ. TLS, SSH, VPN ή ιδιωτικών γραμμών ελεγχόμενης πρόσβασης)

Η ενεργοποίηση της επικοινωνίας θα γίνεται μόνο μέσω θετικών ενεργειών του Διαχειριστή Ασφάλειας Πληροφοριών ή άλλου υπευθύνου που έχει οριστεί

2.6 Λογισμικό

Ο «Δήμος Κιλκίς» χρησιμοποιεί λογισμικό σε όλες τις πτυχές της υπηρεσίας του για να υποστηρίξει το έργο που επιτελούν οι υπάλληλοί του.

Σε όλες τις περιπτώσεις, κάθε λογισμικό απαιτείται να έχει άδεια και ο «Δήμος Κιλκίς» δεν θα εγκρίνει τη χρήση λογισμικού που δεν διαθέτει άδεια.

Αυτό περιλαμβάνει λογισμικό που μπορεί να μεταφορτωθεί ή / και να αγοραστεί από το Internet.

Το λογισμικό ανοιχτού κώδικα, το ελεύθερο λογισμικό και το δωρεάν λογισμικό δεσμεύονται από τις ίδιες πολιτικές και διαδικασίες όπως και το υπόλοιπο λογισμικό.

Ο Διαχειριστής Ασφάλειας Πληροφοριών διατηρεί μητρώο όλων των λογισμικών του «Δήμου Κιλκίς», και θα διατηρεί βιβλιοθήκη αδειών λογισμικού. Το μητρώο πρέπει να περιέχει:

- Τον τίτλος και τον εκδότη του λογισμικού
- Την ημερομηνία και την πηγή της απόκτησης του λογισμικού

- Τη θέση κάθε εγκατάστασης καθώς και τον σειριακό αριθμό του υλικού στο οποίο είναι εγκατεστημένο κάθε αντίγραφο του λογισμικού
- Την ύπαρξη και την θέση αντιγράφων ασφαλείας
- Τον σειριακό αριθμό του προϊόντος λογισμικού
- Λεπτομέρειες και διάρκεια των ρυθμίσεων υποστήριξης για αναβαθμίσεις λογισμικού

Το λογισμικό σε τοπικά δίκτυα ή σε πολλαπλά μηχανήματα χρησιμοποιείται μόνο σύμφωνα με τη σύμβαση άδειας χρήσης.

Το λογισμικό πρέπει να εγκατασταθεί μόνο από την ομάδα IT.

Όλες οι αλλαγές στο λογισμικό πρέπει να εγκριθούν πριν από την εφαρμογή της αλλαγής.

Σε καμία περίπτωση προσωπικό ή ανεπιθύμητο λογισμικό δεν θα πρέπει να φορτώνεται στο «Δήμο Κιλκίς», (αυτό περιλαμβάνει προγράμματα screen savers, παιχνίδια και wallpapers κλπ.), καθώς υπάρχει σοβαρός κίνδυνος εισαγωγής ενός ιού.

Το λογισμικό δεν πρέπει να αλλάζεται ή να μεταβάλλεται από οποιονδήποτε χρήστη εκτός εάν υπάρχει σαφής υπηρεσιακή ανάγκη.

Οποιοσδήποτε χρήστης του «Δήμου Κιλκίς» ο οποίος πραγματοποιεί, αποκτά ή χρησιμοποιεί μη εξουσιοδοτημένα αντίγραφα λογισμικού, θα έχει πειθαρχικές κυρώσεις ανάλογα με τις περιστάσεις. Ο «Δήμος Κιλκίς» δεν εγκρίνει την παράνομη αλληλεπικάλυψη λογισμικού και δεν θα το ανεχτεί.