ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μελέτη και υλοποίηση μέτρων συμμόρφωσης σε εταιρία ως προς το πρότυπο ISO-27001 και εναρμόνισης με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης

Των φοιτητών:

Γεώργιος Μουντζούρογλου
Αρ. Μητρώου: 920297

Βασίλειος Γιαννιώτης
Αρ. Μητρώου: 920320

Επιβλέπων καθηγητής

Γιακουστίδης Κωνσταντίνος

Θεσσαλονίκη 2019

ΠΡΟΛΟΓΟΣ

Ήδη από τις 25 Μαΐου 2018 ισχύει, με υποχρεωτική εφαρμογή σε όλους οργανισμούς της Ευρωπαϊκής Ένωσης, ο νέος κανονισμός γενικής προστασίας δεδομένων (General Data Protection Regulation – GDPR). Μ' αυτόν τον κανονισμό τυποποιούνται οι κανόνες στην ΕΕ, ώστε να εξασφαλίζεται αυστηρότερος έλεγχος όλων των οργανισμών που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, με αυστηρά μάλιστα πρόστιμα για τη μη συμμόρφωση.

Σε κάθε οργανισμό - εταιρία το ζήτημα της ασφάλειας πληροφοριών είναι εξόχως σημαντικό. Η κρισιμότητα αυτή απορρέει από το πόσο σημαντικές είναι οι πληροφορίες τις οποίες διαχειρίζεται η εταιρία. Το GDPR ενθαρρύνει τη χρήση συστημάτων πιστοποίησης, όπως το ISO 27001, για να επιδείξει ότι ο κάθε οργανισμός διαχειρίζεται ενεργά την ασφάλεια των δεδομένων του, σύμφωνα με τις διεθνείς βέλτιστες πρακτικές.

Αυτός ακριβώς ο συγκερασμός του Ευρωπαϊκού Κανονισμού (GDPR), με ένα διεθνές πρότυπο βέλτιστων πρακτικών για την ασφάλεια των πληροφοριών όπως το (ISO-27001) είναι κι ο σκοπός της πτυχιακής μας εργασίας.

ΠΕΡΙΛΗΨΗ

Το κρίσιμο θέμα της ασφάλειας των ψηφιακών συστημάτων αποτελεί αναμφισβήτητα κεντρικό αντικείμενο ενδιαφέροντος μιας εταιρίας στις μέρες μας. Όπως γίνεται αμέσως κατανοητό δίχως την σωστή διαχείριση ασφάλειας η οποιαδήποτε εταιρία μπορεί να βρεθεί αντιμέτωπη με μια σειρά κινδύνων, που μπορούν να οδηγήσουν σε δυσλειτουργία της και κατά συνέπεια σε μικρή ή μεγαλύτερη απώλεια της αξιοπιστίας της, της φήμης της, του πελατολογίου της κ.τ.λ. κι ίσως ακόμα σε νομικές περιπέτειες και δικαστικές κυρώσεις. Έτσι οι εταιρίες δαπανούν σημαντικά ποσά για την ασφάλεια των πληροφοριών που διαχειρίζονται και εγκαθιστούν διάφορες τεχνολογικές λύσεις όπως συστήματα firewall, antivirus κ.α. Πέρα όμως από τις διάφορες αυτές λύσεις η διαχείριση της ασφάλειας πληροφοριών περιλαμβάνει κι άλλες συνιστώσες όπως τα άτομα και τις διαδικασίες.

Στη πτυχιακή μας εργασία παρουσιάζονται κεντρικά στοιχεία τόσο του διεθνούς προτύπου ISO-27001 όσο του Ευρωπαϊκού Κανονισμού GDPR πάνω στην ασφάλεια γενικά της πληροφορίας που διαχειρίζεται μια εταιρία που δραστηριοποιείται στο χώρο της πληροφορικής και συγκεκριμένα στην παραγωγή ολοκληρωμένων πληροφοριακών συστημάτων (ΟΠΣ), αλλά και της ασφάλειας των προσωπικών δεδομένων ειδικότερα. Παρουσιάζουμε έτσι μια μελέτη σε μια υπαρκτή εταιρία και σε ένα εν λειτουργία «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών» - ISMS (Information Security Management System). Η υλοποίηση ο έλεγχος κι η συνεχής βελτίωση ενός ISMS με βάση τις οδηγίες και τις απαιτήσεις του προτύπου (ISO-27001) και του κανονισμού (GDPR) καθιστά την εταιρία επικαιροποιημένη / εναρμονισμένη και σύννομη σύμφωνα με το ισχύον νομικό πλαίσιο τόσο σε εγχώριο όσο και σε ευρωπαϊκό επίπεδο, ενισχύοντας και διασφαλίζοντας τη θέση της έναντι του ανταγωνισμού ως προς την ασφάλεια των πληροφοριών και των πνευματικών της δικαιωμάτων.

ABSTRACT

The critical issue of the security of digital systems is undoubtedly the central subject of interest of a company nowadays. As is immediately understood without proper security management, any company may be confronted with a number of risks that may lead to its malfunction and consequently to a small or greater loss of its credibility, reputation, clientele and perhaps still in legal adventures and judicial penalties. Therefore, companies spend considerable amounts of money on information security that manages and installs various technology solutions such as firewall, antivirus, etc. Apart from these different technological solutions, information security management also includes other components such as individuals and procedures.

In our dissertation we present key elements of both the international standard ISO-27001 and the European GDPR Regulation on the security of information in general, managed by a company operating in the field of information technology, namely the production of integrated information systems (IIS) and personal data security in particular. We present a study of an "Information Security Management System" (ISMS) in an operational active company. The implementation and the continuous improvement of an ISMS based on the guidelines and requirements of the standard (ISO-27001) and the Regulation (GDPR) brings the company up-to-date / harmonized and legal in accordance with the current legal framework both in domestic and in European level by strengthening and safeguarding its position vis-à-vis competition on the security of information and its intellectual property rights.

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα θέλαμε να ευχαριστήσουμε τον υπεύθυνο καθηγητή μας κ. Γιακουστίδη Κωνσταντίνο για την καθοδήγηση, βοήθεια και τη γενικότερη συμβολή του στην ολοκλήρωση της πτυχιακής μας εργασίας αλλά κυρίως για την ανάθεση της και την εμπιστοσύνη του από την πρώτη στιγμή.

Στη συνέχεια ευχαριστούμε τις οικογένειές μας για την στήριξη που μας παρείχαν αλλά και για την προτροπή τους στο να πιστέψουμε στην συνέχεια και ολοκλήρωση αυτής της ομολογουμένως μακρόχρονης προσπάθειας.

Τέλος αφιερώνεται με αγάπη στους γονείς μας ζώντες κι εκλιπόντες.

ΠΕΡΙΕΧΟΜΕΝΑ

Ευρετήριο σχημάτων

Ευρετήριο πινάκων

ΕΙΣΑΓΩΓΗ

Αρχικά στην πτυχιακή μας εργασία επιχειρείται μία εισαγωγή στην αλληλεπίδραση του διεθνούς προτύπου ISO-27001 και του Ευρωπαϊκού κανονισμού GDPR. Στη συνέχεια θα γίνει συνοπτική παρουσίαση της ανάλυσης των κινδύνων που διατρέχει μια σύγχρονη εταιρία που δραστηριοποιείται όπως προαναφέρθηκε στο χώρο της παραγωγής ολοκληρωμένων πληροφοριακών συστημάτων, όπως και τα αποδεκτά από την εταιρία όρια κρισιμότητας αυτών. Στη συνέχεια θα γίνει αναφορά στα μέτρα ασφαλείας και πρόληψης, τις μεθόδους οργάνωσης που ορίστηκαν και υλοποιήθηκαν προκειμένου η εν λόγω εταιρία να πιστοποιηθεί και να βελτιώσει τις εσωτερικές της διαδικασίες και να θωρακιστεί από πιθανή απώλεια δεδομένων προσωπικού ή μη χαρακτήρα, καθώς επίσης και του αναπτυσσόμενου κώδικα του λογισμικού που αποτελεί το κύριο περιουσιακό στοιχείο της εταιρίας. Ως αποτέλεσμα των προσπαθειών αυτών θεωρούμε πως επιτεύχθηκε σε μεγάλο βαθμό η αναβάθμιση των παρεχομένων υπηρεσιών προς τους πελάτες αλλά και η διατήρηση και επαύξηση της αξιοπιστίας της εταιρίας στο υπάρχον αλλά και στο εν δυνάμει πελατολόγιό της.

Στην πορεία της διπλωματικής εργασίας, θα αναπτυχθούν διεξοδικά τα παραπάνω θέματα και οι τρόποι που επιλέχθηκαν προς την υλοποίηση των μέτρων ασφαλείας.

ΚΕΦΑΛΑΙΟ 1
Το πρότυπο ISO27001:2013 και ο κανονισμός γενικής προστασίας δεδομένων (General Data Protection Regulation – GDPR).

ΕΙΣΑΓΩΓΗ

Στο ραγδαία εξελισσόμενο τομέα της ψηφιακής τεχνολογίας και του διαδικτύου δημιουργείται ολοένα και πιο επιτακτική η ανάγκη για την προστασία των ανταλλασσόμενων πληροφοριών. Τα συστήματα που αναπτύσσονται για το σκοπό αυτό είναι πλέον πολυάριθμα και ποικίλα. Οι χρήστες των συστημάτων αυτών, πολλές φόρες αγνοούν τους κινδύνους που μπορεί να απειλούν τα δεδομένα μιας επιχείρησης ή οργανισμού.

«Οι ταχείες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση έχουν δημιουργήσει νέες προκλήσεις για την προστασία των προσωπικών δεδομένων. Η κλίμακα συλλογής και ανταλλαγής δεδομένων προσωπικού χαρακτήρα έχει αυξηθεί σημαντικά», (οδηγία Ευρωπαϊκής Ένωσης 2016/680)1.

Συνεπάγεται λοιπόν, ότι η προστασία της ιδιωτικότητας αποτελεί πλέον το βασικό διακύβευμα του 21ου αιώνα. Έτσι λοιπόν τα σύγχρονα πληροφοριακά συστήματα καλούνται να διαχειριστούν την ασφάλεια των πληροφοριών (information security management) και τα προβλήματα τα οποία προκύπτουν απ' αυτήν. Η ανάγκη για ασφαλή διαχείριση της πληροφορίας, των συστημάτων και των χρηστών, οδήγησε στη δημιουργία προτύπων ασφαλείας τα οποία καθοδηγούν μια επιχείρηση να εξασφαλίσει ότι τα δεδομένα της είναι ασφαλή. Με τη σειρά τους τα πρότυπα αυτά δημιούργησαν την ανάγκη ελέγχου μια επιχείρησης με σκοπό τη διασφάλιση των δεδομένων τους.

1.1 Πρότυπο ISO27001:2013

Σύμφωνα με την οδηγία 2016/6805 της Ευρωπαϊκής Ένωσης : «Οι ταχείες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση έχουν δημιουργήσει νέες προκλήσεις για την προστασία των προσωπικών δεδομένων. Η κλίμακα συλλογής και ανταλλαγής δεδομένων προσωπικού χαρακτήρα έχει αυξηθεί σημαντικά».

Έτσι λοιπόν το πρότυπο ISO 27001:2013 αναπτύχθηκε με σκοπό την προστασία της πληροφορίας μιας εταιρίας ή ενός οργανισμού λαμβάνοντας υπόψη τις σύγχρονες απαιτήσεις για την εφαρμογή της διατήρησης και της συνεχούς βελτίωσης ενός Συστήματος Διαχείρισης Πληροφοριών. Πρόκειται για ένα διεθνές πρότυπο βάσει του οποίου παρέχονται και περιγράφονται όλες οι βέλτιστες πρακτικές, για την υλοποίηση των απαιτήσεων αυτών και περιλαμβάνει το τρίπτυχο που απαρτίζεται από τις κύριες συνιστώσες ενός ολοκληρωμένου περιβάλλοντος ασφάλειας των πληροφοριών: τους ανθρώπους, τις τηρούμενες και εξελισσόμενες διαδικασίες και την σύγχρονη κάθε φορά τεχνολογία. Οι βασικές αρχές της ασφάλειας των πληροφοριών που το πρότυπο επιχειρεί να διασφαλίσει στηρίζονται σε τρία βασικά χαρακτηριστικά:

Εμπιστευτικότητα (Confidentiality): Διασφάλιση προσπέλασης της πληροφορίας μόνον από σε εξουσιοδοτημένους και έχοντες τα απαραίτητα δικαιώματα.

Ακεραιότητα (Integrity): Διασφάλιση της ακρίβειας και της πληρότητας της πληροφορίας. Ανάπτυξη μεθόδων ασφαλούς επεξεργασίας της πληροφορίας αυτής.

Διαθεσιμότητα (Availability): Διαρκής και απρόσκοπτη προσπέλαση της πληροφορίας κατά το δοκούν σε εξουσιοδοτημένους χρήστες και μόνον.

Το «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών» - ISMS (Information Security Management System), θα πρέπει να παρακολουθείτε συνεχώς αλλά και να επανεξετάζεται ανά τακτά χρονικά διαστήματα ώστε τα τρία παραπά
νω βασικά χαρακτηριστικά της ασφάλειας των πληροφοριών να διατηρούνται πάντα επικαιροποιημένα και συνεπώς αποτελεσματικά. Το πρότυπο ISO 27001:2013 ακολουθεί, όπως και κάθε ISO πρότυπο, τον κύκλο plan-do-check-act (PDCA).

1.2 Κανονισμός γενικής προστασίας δεδομένων (GDPR)

Ο Γενικός Κανονισμός για τα Προσωπικά Δεδομένα (Κανονισμός της Ευρωπαϊκής Ένωσης 2016/679) τέθηκε σε ισχύ το Μάιο του 2018 και αφορά όλες τις επιχειρήσεις και τους δημόσιους ή ιδιωτικούς φορείς που διαχειρίζονται ή επεξεργάζονται προσωπικά δεδομένα πολιτών της Ευρωπαϊκής Ένωσης. Οι

παραπάνω φορείς δύναται να τηρούν στοιχεία χρηστών διαδικτύου αλλά και στοιχεία πελατών. Ο Γενικός Κανονισμός ρυθμίζει ζητήματα επεξεργασίας, διαχείρισης και προστασίας των προσωπικών δεδομένων αλλά και της ελεύθερης κυκλοφορίας αυτών εντός της επικράτειας της Ευρωπαϊκής Ένωσης αλλά και στους σχετιζόμενους με αυτήν.

Πρόκειται για την πιο πρόσφατη και πλέον ενημερωμένη νομοθετική εξέλιξη της Ευρωπαϊκής Ένωσης που στοχεύει στη διαφύλαξη της ασφάλειας και της προστασίας των προσωπικών δεδομένων των φυσικών προσώπων. Η επικαιροποίηση του νομοθετικού πλαισίου λόγω των τεχνολογικών εξελίξεων και της τεράστιας αξίας των πληροφοριών, αποτέλεσε ανάγκη για τη θέσπιση του Γενικού Κανονισμού. Με άλλα λόγια, η νομοθετική αλλαγή ήταν επιβεβλημένη, ώστε να προσαρμοστεί στη σύγχρονη ψηφιακή τεχνολογία, να εδραιωθεί κλίμα εμπιστοσύνης ως προς την ασφάλεια των συναλλαγών και να υπάρχει ενιαία αντιμετώπιση σε όλη την Ευρωπαϊκή Ένωση. Εν κατακλείδι, ορισμένες από τις καινοτομίες που εισάγει ο Γενικός Κανονισμός είναι: ο θεσμός του υπευθύνου προστασίας δεδομένων (*Data Protection Officer*), το δικαίωμα στη λήθη (Right to be Forgotten) και τη φορητότητα (Data Portability), καθώς κι οι αρχές της διαφάνειας και της λογοδοσίας όπως και η υποχρέωση γνωστοποίησης παραβιάσεων προσωπικών δεδομένων. Επίσης, υιοθετήθηκαν σύγχρονες έννοιες της επιστήμης της πληροφορικής, όπως για παράδειγμα η εκτίμηση επιπτώσεων (αντικτύπου) στις περιπτώσεις που η επεξεργασία κρίνεται επικίνδυνη για την ασφάλεια των προσωπικών δεδομένων (data protection impact assessment), η προσέγγιση με βάση τον κίνδυνο (risk-based approach), η προστασία εκ σχεδιασμού και εξ ορισμού (privacy by design, privacy by default), η ασφάλεια δεδομένων ως οργανωτική αρχή κ.λ.π..

ΕΠΙΛΟΓΟΣ

Σύμφωνα με τον Γενικό Κανονισμό υπάρχουν πολλές αναφορές σε συστήματα πιστοποίησης, σφραγίδες και σήματα. Ο Γενικός Κανονισμός ενθαρρύνει τη χρήση συστημάτων πιστοποίησης όπως το ISO 27001 για να επιδείξει ότι ο οργανισμός διαχειρίζεται ενεργά την ασφάλεια των δεδομένων του σύμφωνα με τις διεθνείς βέλτιστες πρακτικές. Ο οργανισμός / εταιρία μπορεί να αναπτύξει ένα ISMS

(σύστημα διαχείρισης ασφάλειας πληροφοριών) που υποστηρίζεται από σωστή ηγεσία, ενσωματωμένο στην κουλτούρα και τη στρατηγική του οργανισμού και το οποίο παρακολουθείται, ενημερώνεται και ελέγχεται συνεχώς. Χρησιμοποιώντας μια διαδικασία συνεχούς βελτίωσης, ο οργανισμός είναι σε θέση να διασφαλίσει ότι το ISMS προσαρμόζεται στις αλλαγές - τόσο στο περιβάλλον όσο και εντός του οργανισμού - για να εντοπίζει συνεχώς και να μειώνει τους κινδύνους.
Για την ανάπτυξη λοιπόν, ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS) θα χρειαστεί να ορίσουμε και να περιγράψουμε τις πολιτικές ασφάλειας της εταιρίας.

ΚΕΦΑΛΑΙΟ 2
Ανάπτυξη πολιτικής ασφάλειας πληροφοριών της εταιρίας.

ΕΙΣΑΓΩΓΗ

Η μελέτη της εργασίας ξεκινάει με τον σχεδιασμό μιας αποδεκτής και θεμιτής από την εταιρία πολιτικής ασφάλειας πληροφοριών, που απαρτίζεται από επιμέρους τμήματα και πολιτικές, οι οποίες ξεκινούν από την αποτύπωση των υφιστάμενων υποδομών και τηρουμένων διαδικασιών και σκοπεύει στην αναβάθμιση όλων αυτών. Η εταιρία ανταποκρινόμενη στις απαιτήσεις της σύγχρονης επιχειρηματικής πραγματικότητας και στοχεύοντας στην προστασία των πληροφοριακών συστημάτων της, αποσκοπώντας πάντα στην απρόσκοπτη και υποδειγματική εξυπηρέτηση των Πελατών της, αποφάσισε να σχεδιάσει και να εγκαταστήσει ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με τις απαιτήσεις του Διεθνούς Προτύπου ISO 27001:2013.
Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών της Εταιρίας καλύπτει τον Σχεδιασμό, Ανάπτυξη, και Υποστήριξη Εφαρμογών Λογισμικού και σχεδιάστηκε σύμφωνα με τις ανάγκες και τις επιδιώξεις της Εταιρίας και τις Νομικές και Κανονιστικές Απαιτήσεις της ισχύουσας Ελληνικής και Κοινοτικής Νομοθεσίας και των τελευταίων κανονισμών (βλ. GDPR).
Η Διοίκηση της εταιρίας δεσμεύεται, για την εφαρμογή και την συνεχή βελτίωση της αποτελεσματικότητας του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, καθώς και για την διάθεση όλων των οικονομικών, τεχνικών και ανθρώπινων πόρων που απαιτούνται για τη λειτουργία του μέσω της Ανασκόπησης από τη Διοίκηση σε ετήσια βάση.

Μέτρο της επιτυχίας του συστήματος, είναι η επίτευξη συγκεκριμένων στόχων και η εμφύσηση εμπιστοσύνης για την ακεραιότητα, και ασφάλεια πληροφοριών σε όλους του εμπλεκόμενους.

Για τους λόγους αυτούς η εταιρία αναπτύσσει και εφαρμόζει Πολιτικές που διασφαλίζουν την ακεραιότητα πληροφοριών από εσωτερικούς και εξωτερικούς κινδύνους. Οι Πολιτικές που εφαρμόζει η εταιρία είναι:

- Πολιτική Ασφάλειας Πληροφοριών
- Πολιτική Αποδεκτής Χρήσης
- Πολιτική Ελέγχου Πρόσβασης
- Πολιτική Ελέγχου Τρίτων Μερών
- Πολιτική Κινητών Συσκευών και Αποθηκευτικών Μέσων
- Πολιτική Απομακρυσμένης Πρόσβασης
- Πολιτική Οργάνωσης Ασφάλειας Πληροφοριών

Πολιτική Ασφάλειας

Η Πολιτική Ασφάλειας της εταιρίας καθορίζει μία σειρά τεχνικών και μη τεχνικών απαιτήσεων που πληρούνται σε όλα τα πληροφοριακά συστήματα της εταιρίας όπως:

- Απόκτηση, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων
- Ασφάλεια Δικτύων
- Ασφάλεια Τερματικών Συσκευών
- Προστασία από Κακόβουλο Λογισμικό
- Διαχείριση Αλλαγών
- Τήρησης & Εγκατάστασης Λογισμικών Αντίγραφα Ασφάλειας
- Αντίγραφα Ασφάλειας
- Ασφάλεια Ηλεκτρονικών Υπηρεσιών
- Κρυπτογράφηση πληροφοριών

Ο καθορισμός των παραπάνω απαιτήσεων διασφαλίζει την ασφαλή λειτουργία και συμμόρφωση με νομικές, κανονιστικές και συμβατικές απαιτήσεις της εταιρίας.

Πολιτική Αποδεκτής Χρήσης

Η Πολιτική Αποδεκτής Χρήσης της εταιρίας καθορίζει τον τρόπο με τον οποίο οι χρήστες αξιοποιούν και χρησιμοποιούν τους υπολογιστικούς και πληροφοριακούς πόρους της εταιρίας.

- Η Διοίκηση της εταιρίας επιθυμεί να παρέχει το μέγιστο δυνατό επίπεδο προστασίας της ιδιωτικής ζωής, αλλά οι χρήστες πρέπει να γνωρίζουν ότι

τα δεδομένα που δημιουργούν στα εταιρικά συστήματα παραμένουν ιδιοκτησία της εταιρίας και ότι αρχεία προσωπικού χαρακτήρα δε θα πρέπει να τηρούνται εντός αυτού. Λόγω της ανάγκης για την προστασία του δικτύου, η διοίκηση δεν μπορεί να εγγυηθεί το απόρρητο των πληροφοριών που είναι αποθηκευμένες σε οποιαδήποτε συσκευή ή μέσο μετάδοσης το οποίο ανήκει στην εταιρία.

- Οι χρήστες του υπολογιστικού και πληροφοριακού συστήματος της εταιρίας είναι υπεύθυνοι για την άσκηση ορθής κρίσης σχετικά με το εύλογο της προσωπικής χρήσης. Οι εργαζόμενοι θα πρέπει να καθοδηγούνται από τη νομοθεσία για τη προσωπική χρήση, και αν υπάρχει κάποια αβεβαιότητα, οι εργαζόμενοι θα πρέπει να συμβουλεύονται προϊστάμενο ή διευθυντή τους.
- Για την ασφάλεια και για λόγους συντήρησης δικτύου, εξουσιοδοτημένο προσωπικού της εταιρίας ενδέχεται να παρακολουθεί τον εξοπλισμό, τα συστήματα και τη μετάδοση των πληροφοριών στο δίκτυο, ανά πάσα στιγμή.
- Η εταιρία διατηρεί το δικαίωμα να επιθεωρεί το δίκτυο και τα συστήματα ελέγχου σε περιοδική βάση για να εξασφαλιστεί η συμμόρφωση με αυτή την πολιτική
- Στις εγκαταστάσεις ασφαλείας οι εργαζόμενοι οφείλουν να τηρούν τάξη στις θέσεις εργασίας τους και να μην αφήνουν στην επιφάνεια αυτών, έγγραφα και εξοπλισμό, που δεν χρησιμοποιούν.
- Στα υπολογιστικά συστήματα, που περιλαμβάνονται στο σύστημα ασφάλειας πληροφοριών, οι χρήστες οφείλουν να τηρούν τάξη στην αρχειοθέτηση των δεδομένων τους και να κρατούν καθαρό desktop, ώστε να διευκολύνεται η χρήση.

Καθορίζονται οι επιτρεπόμενες ή όχι συστημικές και δικτυακές Δραστηριότητες των χρηστών της εταιρία. Η πρόσβαση των χρηστών και ο τρόπος πρόσβασης στις πληροφορίες και τους πόρους του συστήματος σύμφωνα με την Οδηγία Διαβάθμισης Δεδομένων.

Πολιτική Ελέγχου Πρόσβασης

Η Πολιτική Ελέγχου Πρόσβασης ορίζει τον τρόπο με τον οποίο η εταιρία θα ελέγχει την πρόσβαση σε πληροφορίες, υποδομές, χώρους και διαδικασίες, ώστε να εξασφαλίζεται το αποδεκτό επίπεδο εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας των πληροφοριακών συστημάτων.
Η Πολιτική Ελέγχου Πρόσβασης διασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες αποκτούν πρόσβαση σε πόρους της εταιρίας και το πεδίο εφαρμογής της περιλαμβάνει όλους τους χρήστες των πληροφοριακών συστημάτων, συμπεριλαμβανομένων των εξωτερικών συνεργατών και τρίτων μερών τα οποία αποκτούν πρόσβαση σε χώρους, συστήματα ή πληροφορίες της

Η πρόσβαση σε όλες της εκδόσεις του πηγαίου κώδικας (source code) των εφαρμογών της εταιρίας ελέγχεται, τόσο κεντρικά, όσο και στα σημεία στα οποία αυτός αναπτύσσεται.

Πολιτική Ελέγχου Τρίτων Μερών

Η Πολιτική Ελέγχου Τρίτων Μερών έχει ως σκοπό να ελαττώσει τους κινδύνους ασφάλειας πληροφοριών που σχετίζονται με δραστηριότητες που πραγματοποιούνται από τρίτα μέρη, εκτός της εταιρίας. Τέτοιοι κίνδυνοι μπορεί να προκύψουν από την παροχή μη εξουσιοδοτημένης πρόσβασης, την απώλεια της εμπιστευτικότητας πληροφοριών και δεδομένων της εταιρίας, την απώλεια προστασίας της πνευματικής ιδιοκτησίας ή οποιαδήποτε ενέργεια ή αμέλεια τρίτων μερών που θα μπορούσε να προκαλέσει βλάβη στην εμπιστευτικότητα, ακεραιότητα ή διαθεσιμότητα των πόρων της εταιρίας. Για αυτό το λόγο πραγματοποιούνται:

- **Έλεγχοι ασφάλειας (Right to Audit).**
- **Έλεγχοι πρόσβασης** για την αποτροπή μη εξουσιοδοτημένης πρόσβασης στους πληροφοριακούς και άλλους πόρους της εταιρίας από τρίτο πάροχο ή υπεργολάβους, απαιτούνται κατάλληλοι έλεγχοι ασφαλείας.
- **Συμφωνίες εμπιστευτικότητας.**
- **Εξέταση επικινδυνότητας εξωτερικής ανάθεσης.**

- **Αξιολόγηση κινδύνων**
- **Επιλογή ενός τρίτου παρόχου με βάση συγκεκριμένα κριτήρια**

Πολιτική Κινητών Συσκευών και Αποθηκευτικών Μέσων

Η Πολιτική Κινητών Συσκευών και Αποθηκευτικών καθορίζει τους κανόνες τηρούνται για τον έλεγχο των κινητών συσκευών και των αφαιρούμενων αποθηκευτικών μέσων που περιέχουν πληροφορίες της εταιρίας και βρίσκονται είτε εντός, είτε εκτός των υποδομών του.

Πολιτική Απομακρυσμένης Πρόσβασης

Η Πολιτική Απομακρυσμένης Πρόσβασης καθορίζει κανόνες και απαιτήσεις που πληρούνται κατά τη σύνδεση στο δίκτυο της εταιρίας από σημεία εκτός αυτού. Πιο συγκεκριμένα κατά την απομακρυσμένη πρόσβαση τους, οι χρήστες της εταιρίας συνδέονται σε διαφορετικά εικονικά ιδιωτικά δίκτυα (VPN) με την εταιρία και αποκτούν διαφορετικό επίπεδο πρόσβασης, ανάλογα με το ρόλο που έχουν.

Έχουν σχεδιαστεί κανόνες για να ελαχιστοποιούν το ενδεχόμενο έκθεσης της εταιρίας σε ζημιές οι οποίες μπορούν να προκύψουν από τη μη εξουσιοδοτημένη χρήση των πόρων του δικτύου της.

Πολιτική Οργάνωσης Ασφάλειας Πληροφοριών

Η Πολιτική Οργάνωσης Ασφάλειας Πληροφοριών ορίζει το διοικητικό πλαίσιο το οποίο ανέπτυξε η εταιρία σχετικά με:

- Τους ρόλους και τις αρμοδιότητες που αφορούν την ασφάλεια πληροφοριών
- Τη διαχείριση των πόρων της εταιρίας
- Τις απαιτήσεις συμμόρφωσης
- Τα τρίτα μέρη

2.1 Πολιτική ασφάλειας πληροφοριών

Ο σκοπός αυτής της πολιτικής είναι να καθορίσει μία σειρά τεχνικών και μη τεχνικών απαιτήσεων που θα πρέπει να πληρούνται σε όλα τα πληροφοριακά συστήματα της εταιρείας, προκειμένου να διασφαλίζεται η ασφαλής λειτουργία τους και η συμμόρφωση με νομικές, κανονιστικές και συμβατικές απαιτήσεις της εταιρείας. Η πολιτική αυτή εφαρμόζεται σε όλη την εταιρεία και αφορά όλα τα στελέχη και το προσωπικό της εταιρείας.

2.1.1 Υπευθυνότητες

- Η Διοίκηση
- Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών (Υ.Δ.Α.Π.)
- Διαχειριστής Δικτύου και Διαχειριστής Συστημάτων (Administrators)
- Ομάδα Ασφάλειας και Ποιότητας
- Επιβλέποντες Προγραμματιστές
- Χρήστες

2.1.2 Περιγραφή

- **Επισκόπηση Ασφάλειας Πληροφοριακών Συστημάτων**
  - Τα πληροφοριακά συστήματα της εταιρείας περιλαμβάνουν λειτουργικά συστήματα, υποδομές, εφαρμογές, προϊόντα τρίτων προμηθευτών, υπηρεσίες και έγγραφα. Η σχεδίαση και η υλοποίηση του πληροφοριακού συστήματος το οποίο αξιοποιείται για να υποστηρίζει τις επιχειρησιακές απαιτήσεις της εταιρείας είναι κρίσιμα για την ασφάλεια των πληροφοριών που δημιουργούνται, επεξεργάζονται και αποθηκεύονται μέσα σε αυτό.
  - Στα πλαίσια της προστασίας των πληροφοριών, η σχεδίαση των εφαρμογών και των υποδομών της εταιρείας έχει βασιστεί στην αρχή του διαχωρισμού των εφαρμογών, των πληροφοριών/δεδομένων, των δικτύων και των τερματικών σταθμών. Στην παρακάτω εικόνα απεικονίζεται ο τρόπος με τον οποίο δομούνται τα διαφορετικά επίπεδα της υποδομής της εταιρίας.

Σχήμα 1 " Επίπεδα υποδομής εταιρίας "

- Μέσα σε αυτή την υποδομή εφαρμόζεται μία σειρά λογικών και τεχνικών αντιμέτρων ασφάλειας, η οποία προορίζεται να παρέχει προστασία σε κάθε ένα από αυτά τα επίπεδα, ξεκινώντας από τη δικτυακή υποδομή, συνεχίζοντας στις τερματικές συσκευές των χρηστών και καταλήγοντας στις εφαρμογές και τα δεδομένα του πληροφοριακού συστήματος.

- **Απόκτηση, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων**
  - Απόκτηση Πληροφοριακών Συστημάτων
    - Η απόκτηση και η ενσωμάτωση στην υποδομή νέων πληροφοριακών ή/και υπολογιστικών συστημάτων θα πρέπει να πραγματοποιείται με ιδιαίτερη φροντίδα, ώστε να μην επιτρέπει τη δημιουργία απειλών προς το επίπεδο ασφάλειας των συστημάτων και πληροφοριών της εταιρείας και να διασφαλίζει τη συμμόρφωση με τις πολιτικές και τις διαδικασίες ασφάλειας που έχουν εγκριθεί.
    - Κατά την απόκτηση πληροφοριακών συστημάτων θα πρέπει να ακολουθούνται όλα όσα υπαγορεύονται, σχετικά με την διαχείριση αλλαγών και την λήψη και επαναφορά αντιγράφων ασφάλειας, στην παρούσα πολιτική.
    - Ειδική μέριμνα πρέπει να λαμβάνεται πριν την απόκτηση ενός νέου συστήματος, αλλά και κατά τη διάρκεια της λειτουργίας και της απομάκρυνσης / παύσης της λειτουργίας του. Συγκεκριμένα, κατά την απόκτησή του θα πρέπει να λαμβάνονται υπόψη τα παρακάτω:

- Τρέχουσες και μελλοντικές απαιτήσεις σε επεξεργαστική ισχύ, χωρητικότητα ή άλλα χαρακτηριστικά που ενδέχεται να επηρεάσουν τα τεχνικά χαρακτηριστικά του συστήματος
- Τυχόν αλλαγές/αστάθειες που ενδέχεται να προκαλέσει η ένταξη αυτού του συστήματος στην υποδομή της εταιρείας

❖ Κατά τη διάρκεια της λειτουργίας των πληροφοριακών συστημάτων, θα πρέπει να εξετάζεται και να εξασφαλίζονται τα παρακάτω:

- η ακεραιότητα της επεξεργασίας, είτε μέσω της ανίχνευσης και αποφυγής λαθών κατά την εισαγωγή δεδομένων στα συστήματα, είτε μέσω του εντοπισμού σφαλμάτων κατά την αποθήκευση ή την επεξεργασία των δεδομένων
- η εμπιστευτικότητα των συναλλαγών, όπου είναι εφικτό μέσω κρυπτογραφικών μεθόδων μετάδοσης δεδομένων
- η ασφάλεια των αρχείων συστήματος, μέσω του ελέγχου των αλλαγών σε αρχεία ρυθμίσεων
- ο έλεγχος και η παρακολούθηση των ενεργειών που πραγματοποιούνται από εξωτερικούς συνεργάτες
- ο καθορισμός και η πλήρωση των τεχνικών απαιτήσεων και η κατάλληλη ρύθμιση/παραμετροποίηση των συστημάτων, προκειμένου να εξασφαλίζεται και, όπου είναι δυνατό, η βελτίωση της αποδοτικότητας των συστημάτων.

➢ Διαχείριση Αλλαγών

❖ Μετά την απόκτηση νέου εξοπλισμού ή νέων συστημάτων, θα απαιτηθεί η πραγματοποίηση μίας σειράς αλλαγών σε διάφορα σημεία των νέων συστημάτων. Οι αλλαγές αυτές, ανεξάρτητα από το σημείο εφαρμογής ή τη μορφή τους θα πρέπει να πραγματοποιούνται σύμφωνα με όσα περιγράφονται στη διαδικασία διαχείρισης αλλαγών και θα πρέπει να είναι σύμφωνα με τις απαιτήσεις διαχείρισης αλλαγών οι οποίες παρατίθενται στην παρούσα πολιτικής.

❖ Η τεχνική τεκμηρίωση κάθε αλλαγής θα πρέπει να περιλαμβάνει μία σειρά ελέγχων αποδοχής για τα νέα συστήματα και τους ελέγχους.

- ❖ Θα πρέπει να πραγματοποιούνται έλεγχοι συμμόρφωσης για να διασφαλιστεί ότι τα νέα συστήματα είναι σύμφωνα με τα πρότυπα και τις διεθνείς πρακτικές που έχουν υιοθετηθεί στις υποδομές της εταιρείας.
- ❖ Αλλαγές σε συστήματα τα οποία βρίσκονται σε παραγωγική λειτουργία ΔΕΝ θα πρέπει να έχουν σημαντικό αντίκτυπο στις επιχειρησιακές, διοικητικές και λειτουργικές δραστηριότητες της εταιρείας, επομένως θα πρέπει να λαμβάνεται ιδιαίτερη μέριμνα όσον αφορά την ώρα και την περίοδο που πραγματοποιούνται αυτές οι αλλαγές.

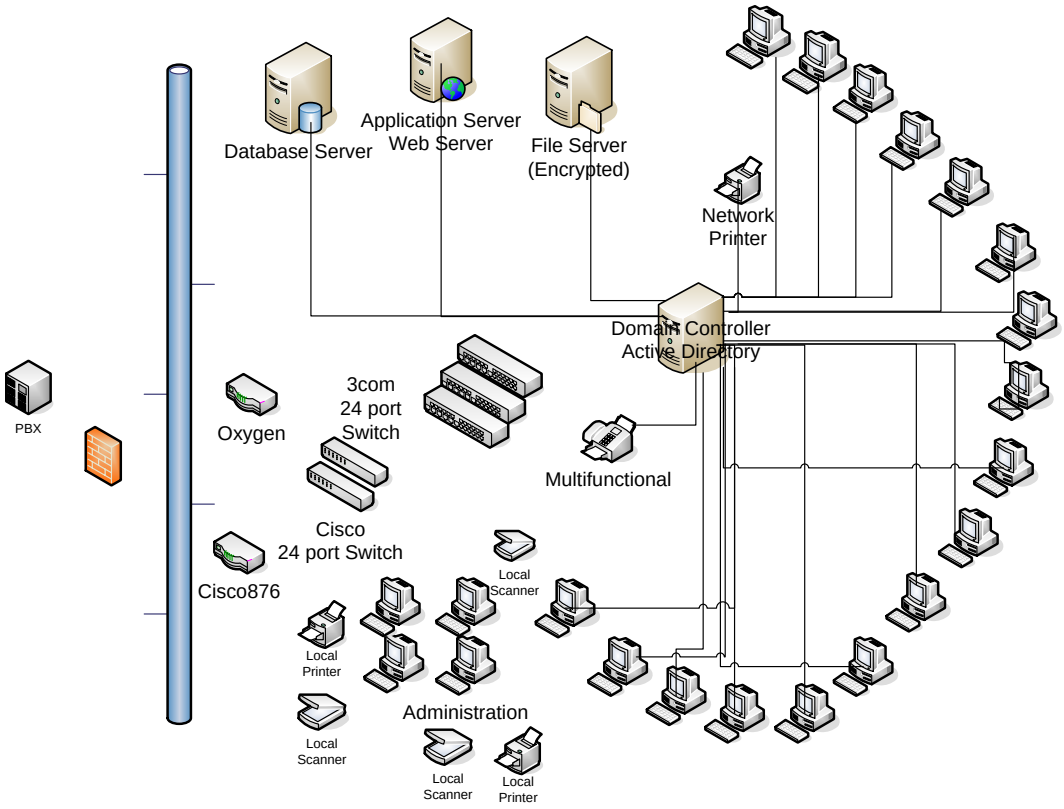
- ➢ Τερματισμός Λειτουργίας
  - ❖ Ειδική μέριμνα θα πρέπει να λαμβάνεται κατά την απομάκρυνση ή παύση λειτουργίας ενός συστήματος ή ενός μέρους εξοπλισμού, ώστε να διασφαλίζεται η συνέχιση των δραστηριοτήτων της εταιρείας και η ακεραιότητα και εμπιστευτικότητα των πληροφοριών που σχετίζονται με το υπό απομάκρυνση σύστημα.
  - ❖ Σε κάθε περίπτωση οι Διαχειριστές Δικτύου και Συστημάτων, σε συνεργασία με τον Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών, θα πρέπει να διασφαλίζουν ότι δεν παραμένουν διαβαθμισμένα δεδομένα ή πληροφορίες στο σύστημα και, εφόσον είναι απαραίτητο, ο εξοπλισμός θα πρέπει να καταστρέφεται σύμφωνα με την Οδηγία Καταστροφής Δεδομένων.

- ➢ Συντήρηση Συστημάτων
  - ❖ Όλα τα συστήματα θα πρέπει να συντηρούνται σε τακτική βάση, σύμφωνα με τις απαιτήσεις και τις προδιαγραφές του κατασκευαστή κάθε μέρους εξοπλισμού.
  - ❖ Οι εργασίες συντήρησης θα πρέπει να πραγματοποιούνται μόνο από εξουσιοδοτημένο προσωπικό και θα πρέπει να καταγράφονται τυχόν σφάλματα που είτε έγιναν, είτε ενδέχεται να προκύψουν, μαζί με τις σχετικές ενέργειες πρόληψης ή επιδιόρθωσης.
  - ❖ Οι υπάλληλοι που είναι επιφορτισμένοι με τη συντήρηση των συστημάτων έχουν τη δικαιοδοσία να μεταφέρουν εκτός των χώρων

επεξεργασίας τον εξοπλισμό, εφόσον αυτό απαιτείται για την πλήρωση των καθηκόντων τους. Σε κάθε περίπτωση θα πρέπει να είναι ενημερωμένοι η Ομάδα Ασφάλειας και Ποιότητας, πριν την μεταφορά του εξοπλισμού εκτός του χώρου επεξεργασίας.

- ❖ Η επιστροφή των συστημάτων / εξοπλισμών θα πρέπει να ελέγχεται και θα πρέπει να τηρείται ιδιαίτερη φροντίδα κατά τη μεταφορά του εξοπλισμού εκτός των χώρων επεξεργασίας.

- **Ασφάλεια Δικτύων**
  - ➢ Το πρώτο λογικό επίπεδο ασφάλειας πληροφοριών της εταιρείας είναι το δίκτυό της. Η δομή του δικτύου της εταιρείας και τα μέτρα προστασίας τα οποία λαμβάνονται στο επίπεδο δικτύου απεικονίζονται στο παρακάτω σχήμα:



Σχήμα 2 " Δομή δικτύου εταιρίας "

Το εσωτερικό εταιρικό δίκτυο (intranet) της εταιρίας όπως αυτό προκύπτει και από το διάγραμμα αποτελείται από:

- 4 Servers

Domain Controller (Master) - File Server
Domain Controller (Back up)
Database Server
Application Web Server

- 19 Η/Υ οι οποίοι συνδέονται στο Domain Controller της εταιρίας και διέπονται από την πολιτική του Domain (Group Policy)
- Καταγραφικό με δύο κάμερες που ελέγχουν την πρόσβαση στο χώρο της εταιρίας.
- 1 Δικτυακό εκτυπωτή
- 3 patch panels για την εσωτερική δομημένη καλωδίωση της εταιρίας
- 2 Switches 24 port
  Cisco
  3Com
- 2 modem routers (όχι με δική μας διαχείριση)
  Oxygen
  Cisco 876
- Firewall (next generation).
- Τηλεφωνικό Κέντρο με Fax Server.

Στο εσωτερικό εταιρικό δίκτυο υπάρχει εγκατεστημένος Domain Controller με Active Directory για την πιστοποίηση (authentication) και την εξουσιοδότηση (authorization) των χρηστών του δικτύου και την πρόσβαση στους διαθέσιμους πόρους του δικτύου ανάλογα με τα δικαιώματα που του έχουν αποδοθεί. Για τη διασφάλιση της συνεχόμενης πρόσβασης και αδιάλειπτης χρήσης των πόρων του δικτύου υπάρχει Back up Domain Controller, για την περίπτωση που ο βασικός Domain Controller δεν θα είναι διαθέσιμος, η ενεργοποίηση του γίνεται αυτόματα. Τα modem routers συνδέονται με το firewall, ώστε να διασφαλίζεται η επικοινωνία στο εσωτερικό δίκτυο και να διαχωρίζεται από το εξωτερικό.
Στο firewall (next generation) εκτός από το "παραδοσιακό" φιλτράρισμα, για την ασφάλεια του εσωτερικού δικτύου τρέχουν χαρακτηριστικά ασφαλείας όπως IPS (Intrusion Prevention System), IDS (Intrusion Detection System) και Content Filtering.

- Ασφάλεια δρομολογητών

- ❖ Οι κωδικοί πρόσβασης των δρομολογητών αλλάζουν από τους διαχειριστές του παρόχου, σύμφωνα με την πολιτική ασφαλείας του.
- ❖ Το λειτουργικό σύστημα των δρομολογητών θα πρέπει να λειτουργεί με την τελευταία έκδοση η οποία υποστηρίζεται από τον κατασκευαστή και δεν υπάρχουν γνωστές ευπάθειες για τις οποίες δεν έχει ανακοινωθεί διόρθωση (patch) από τον κατασκευαστή
- ❖ Οι λίστες πρόσβασης έχουν ρυθμιστεί ώστε να επιτρέπουν μόνο τα πρωτόκολλά τα οποία είναι απαραίτητα για τις επικοινωνίες που πραγματοποιούνται στα πλαίσια επιχειρησιακών αναγκών. Τα μη χρησιμοποιούμενα πρωτόκολλα θα πρέπει να μην είναι προσβάσιμα.
- ❖ Τα αρχεία ρυθμίσεων, όταν αποθηκεύονται εκτός του εξοπλισμού θα πρέπει να βρίσκονται σε ασφαλή τοποθεσία. Μόνο εξουσιοδοτημένο προσωπικό με επιχειρησιακή ανάγκη θα πρέπει να έχει πρόσβαση σε αυτά.
- ❖ Οι δρομολογητές θα είναι φυσικά προσβάσιμοι μόνο από εξουσιοδοτημένο προσωπικό, όπως επίσης και η λογική πρόσβαση στους δρομολογητές θα επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.
- ❖ Οι δρομολογητές θα πρέπει να έχουν ενεργοποιημένες μόνο τις απαιτούμενες υπηρεσίες. Όλες οι άλλες υπηρεσίες θα πρέπει να είναι απενεργοποιημένες.

- ➢ Ασφάλεια Firewalls
  - ❖ Το Firewall της εταιρείας θα πρέπει να βρίσκεται σε διάταξη υψηλής διαθεσιμότητας, με τρόπο που να διασφαλίζει το διαχωρισμό των δικτύων όπως περιγράφεται ακριβώς στην προηγούμενη παράγραφο.
  - ❖ Θα πρέπει να χρησιμοποιούνται ασφαλείς κωδικοί για την πρόσβαση στα Firewalls. Οι κωδικοί αυτοί θα τροποποιούνται κάθε φορά που αλλάζει το προσωπικό που χειρίζεται κάποιο Firewall ή κάθε τριάντα (30) ημέρες.
  - ❖ Μόνο εξουσιοδοτημένο προσωπικό θα έχει φυσική ή λογική πρόσβαση στα Firewalls.
- ➢ Ρολόγια συγχρονισμού

- ❖ Τα ρολόγια συγχρονισμού όλων των συστημάτων επεξεργασίας πληροφορίας θα πρέπει να συγχρονίζονται με μια έμπιστη πηγή παροχής ώρας.
- ❖ Για τον συγχρονισμό όλων των ρολογιών θα πρέπει να χρησιμοποιείται το πρωτόκολλο NTP (Network Time Protocol).
- ❖ Όταν ένας υπολογιστής ή κάποιο μέρος δικτυακού εξοπλισμού έχει τη δυνατότητα να χρησιμοποιηθεί ως ρολόι, αυτό το ρολόι θα πρέπει να έχει ρυθμιστεί στην τοπική ώρα.

➢ Ασφάλεια Καλωδίων

- ❖ Οι δικτυακές καλωδιώσεις είναι προστατευμένες από μη εξουσιοδοτημένες παρεμβολές ή βλάβες, όταν περνούν από δημοσίως προσβάσιμα σημεία της υποδομής της εταιρείας.
- ❖ Τα καλώδια ρεύματος είναι διαχωρισμένα από τα καλώδια δικτύου προκειμένου να αποφεύγονται παρεμβολές κατά μετάδοση δεδομένων.
- ❖ Θα πρέπει να χρησιμοποιείται ειδική σήμανση στα καλώδια, προκειμένου να αποφευχθεί ο κίνδυνος σφαλμάτων κατά τον χειρισμό των καλωδίων.
- ❖ Η πρόσβαση σε σημεία όπου καταλήγουν τα καλώδια θα πρέπει να είναι προστατευμένα και σε αυτά να έχει πρόσβαση μόνο εξουσιοδοτημένο προσωπικό.

- **Ασφάλεια Τερματικών Συσκευών**

➢ Το λειτουργικό σύστημα το οποίο χρησιμοποιείται στις τερματικές συσκευές θα πρέπει να έχει παραμετροποιηθεί με όλες τις διαθέσιμες διορθώσεις που έχουν δοθεί από τον κατασκευαστή. Τα αποδεκτά λειτουργικά συστήματα τα οποία μπορούν να εγκαθίστανται σε τερματικές συσκευές είναι τα παρακάτω:

- ❖ Windows 10 Pro

➢ Μόνο εξουσιοδοτημένοι χρήστες μπορούν να πραγματοποιούν διαχειριστικές εργασίες στους σταθμούς εργασίας.

- Οι υπηρεσίες και οι εφαρμογές οι οποίες δε χρησιμοποιούνται στις τερματικές συσκευές θα πρέπει να απενεργοποιούνται.
- Το λογισμικό το οποίο εγκαθίσταται σε κάθε τερματική συσκευή θα πρέπει να έχει την κατάλληλη άδεια χρήσης (license).
- Θα πρέπει σε κάθε τερματική συσκευή να είναι ενεργοποιημένες επιλογές καταγραφής (logging).
- Οι σταθμοί εργασίας, όταν βρίσκονται συνδεδεμένοι στο εσωτερικό δίκτυο της εταιρείας έχουν συγκεκριμένη διεύθυνση δικτύου (IP Address), η οποία δίδεται από τους Διαχειριστές Δικτύου και Συστημάτων.
- Οι απαιτήσεις ασφάλειας των κωδικών πρόσβασης που χρησιμοποιούνται στις τερματικές συσκευές εξαρτώνται από το ρόλο που επιτελεί κάθε συσκευή και θα πρέπει να ρυθμίζονται σύμφωνα με τις απαιτήσεις που καθορίζονται στην Πολιτική Ελέγχου Πρόσβασης.
- Οι λογαριασμοί με διαχειριστική πρόσβαση (π.χ. root για το λειτουργικό σύστημα Linux και Administrator για το λειτουργικό σύστημα Windows) θα πρέπει να είναι παραμετροποιημένοι με ασφαλή τρόπο.
- Η πρόσβαση σε αρχεία και φακέλους κάθε τερματικής συσκευής θα πρέπει να σχετίζεται με τη ταυτότητα του χρήστη, με την οποία θα ορίζονται τα δικαιώματα του χρήστη (read, write, execute).

- **Προστασία από Κακόβουλο Λογισμικό**
  - Οι χρήστες θα πρέπει να είναι ενημερωμένοι για τους κινδύνους που σχετίζονται με το κακόβουλο λογισμικό όπως είναι οι ιοί υπολογιστών, τα network worms,Trojan horses και logic bombs.
  - Οι Διαχειριστές Δικτύου και Συστημάτων της εταιρείας θα πρέπει να εφαρμόζουν αντίμετρα τα οποία να αποτρέπουν, ανιχνεύουν και αφαιρούν κακόβουλο λογισμικό.
  - Υπάρχει εγκατεστημένο σε όλους τους υπολογιστές της εταιρείας λογισμικό εντοπισμού και αντιμετώπισης κακόβουλου λογισμικού, το οποίο ενημερώνεται αυτόματα με τις νεότερες εκδόσεις και υπογραφές.

- Η εγκατάσταση και η ενημέρωση εργαλείων ανίχνευσης και καταπολέμησης κακόβουλου λογισμικού θα πρέπει να πραγματοποιείται σε όλες τις τερματικές συσκευές, οι οποίες θα πρέπει να σαρώνονται σε τακτική βάση.
- Αρχεία ή αφαιρούμενα μέσα αποθήκευσης, αλλά και πληροφορίες που λαμβάνονται από το δίκτυο θα πρέπει να εξετάζονται για να διαπιστωθεί η ύπαρξη ή μη κακόβουλου λογισμικού πριν εισέλθουν στην υποδομή της εταιρείας.
- Τα επισυναπτόμενα στην ηλεκτρονική αλληλογραφία των χρηστών αρχεία θα πρέπει να ελέγχονται για να διαπιστωθεί η ύπαρξη ή μη κακόβουλου λογισμικού.

- **Διαχείριση Αλλαγών**
  - Για την αρμονική συνέχιση των λειτουργιών της εταιρείας κατά την πραγματοποίηση αλλαγών, είναι απαραίτητη η θέσπιση μίας σειράς κανόνων που θα πρέπει να ακολουθούνται κατά τη διάρκεια όλων των ειδών αλλαγών, στις οποίες περιλαμβάνονται οι παρακάτω:

    - Εγκατάσταση, αλλαγή, αφαίρεση ή μετακίνηση λογισμικού (hardware)
    - Εγκατάσταση, επιδιόρθωση (patching), αναβάθμιση ή αφαίρεση προϊόντων λογισμικού, συμπεριλαμβανομένων λειτουργικών συστημάτων, έτοιμων πακέτων λογισμικού ή εφαρμογών που έχουν αναπτυχθεί από την εταιρία.
    - Αλλαγές σε βάσεις δεδομένων ή αρχεία που περιέχουν δεδομένα
    - Αλλαγές σε εφαρμογές της εταιρείας ή ενσωμάτωση νέων συστημάτων και η αφαίρεση ξεπερασμένων συστημάτων που δε χρησιμοποιούνται.
    - Προγραμματισμένες αλλαγές στην υποδομή και τα στοιχεία υποδομής
    - Αλλαγές που ενδέχεται να προκύψουν για να καλύψουν επιχειρησιακές, διοικητικές και λειτουργικές απαιτήσεις της εταιρείας.
  - Εκτός των παραπάνω, υπάρχει μία σειρά αλλαγών για τις οποίες δεν απαιτείται η κεντρική αναφορά και παρακολούθηση τους. Αυτές οι αλλαγές περιλαμβάνουν:

- ❖ Αλλαγές σε μη παραγωγικά στοιχεία της υποδομής ή πόρους που δεν βρίσκονται σε παραγωγική λειτουργία
- ❖ Αλλαγές που πραγματοποιούνται στα πλαίσια καθημερινών διαχειριστικών καθηκόντων, όπως η αλλαγή κωδικών πρόσβασης, η τροποποίηση χρηστών, η επανεκκίνηση εξοπλισμού, κ.α.

- ➢ Κάθε αλλαγή που πραγματοποιείται στα συστήματα της εταιρίας θα πρέπει να πραγματοποιείται σε δύο διακριτά στάδια, τα οποία είναι:
  - ❖ Στάδιο Προετοιμασίας: Σε αυτό το στάδιο περιλαμβάνονται οι διαδικασίες έγκρισης, η ανάλυση της αναγκαιότητας κάθε αλλαγής, η εκτίμηση της επικινδυνότητας που σχετίζεται με την αλλαγή και η σχεδίαση των εργασιών που θα ακολουθηθούν για τη πραγματοποίηση των αλλαγών
  - ❖ Στάδιο Εφαρμογής: Σε αυτό το στάδιο πραγματοποιείται η αλλαγή, ο έλεγχος της ορθότητας της και ο έλεγχος ακεραιότητας των επηρεαζόμενων λειτουργιών ή / και συστημάτων.
- ➢ Για να αποφασιστεί η προτεραιότητα κάθε αλλαγής και κατ' επέκταση να οριστεί ο χρόνος υλοποίησης της, έχουν οριστεί τρία επίπεδα αλλαγών, στα οποία θα πρέπει να εντάσσεται κάθε αλλαγή. Τα επίπεδα αυτά είναι:
  - ❖ Μικρές Αλλαγές (Minor). Αλλαγές που μπορεί να επηρεάσουν χαμηλής κρισιμότητας υπηρεσίας ή ενδέχεται να έχουν ασήμαντες συνέπειες.
  - ❖ Μεγάλες Αλλαγές (Major). Αλλαγές που ενδέχεται να έχουν μεγάλο αντίκτυπο στη λειτουργία συστημάτων ή μπορεί να επηρεάσουν μεγάλο πλήθος συστημάτων της εταιρείας ή μπορεί να επηρεάσουν συστήματα υψηλής κρισιμότητας.
  - ❖ Επείγουσες Αλλαγές (Emergency). Αλλαγές που μπορεί να προκύψουν και να ζητηθούν ως επείγουσα απαίτηση.
- ➢ Η προτεραιότητα και οι απαιτήσεις που σχετίζονται με κάθε αλλαγή εξαρτώνται από τον τύπο της αλλαγής, και το επίπεδο επικινδυνότητας της αλλαγής.
  - ❖ Μικρές Αλλαγές. Οι αλλαγές αυτές δεν απαιτούν εξουσιοδότηση και δεν χρειάζονται επίσημη έγκριση για την υλοποίηση τους. Οι αλλαγές

αυτές θα πρέπει να παρακολουθούνται, αλλά θα προχωρήσουν άμεσα στη φάση υλοποίησης από τους Διαχειριστές Δικτύου και Συστημάτων.

- ❖ Μεγάλες Αλλαγές (Major). Για την πραγματοποίηση των αλλαγών αυτών θα πρέπει να είναι ενήμερο το σύνολο του προσωπικού και θα απαιτείται έγκριση της Διοίκησης για την πραγματοποίησή τους.
- ❖ Επείγουσες Αλλαγές (Emergency). Οι αλλαγές αυτές δεν απαιτείται να ακολουθήσουν την τυπική διαδικασία εγκρίσεων και παίρνουν μεγαλύτερη προτεραιότητα υλοποίησης από όλες τις άλλες αλλαγές.

- ➢ Η εγκατάσταση διορθωτικών πακέτων (patches) στο λογισμικό των συστημάτων της εταιρείας θα πρέπει να πραγματοποιείται σύμφωνα με τα όσα ορίζονται στην παρούσα πολιτική για τη διαχείριση αλλαγών και σύμφωνα με την διαδικασία διαχείρισης αλλαγών. Κάθε Επιβλέπων Προγραμματιστής είναι υπεύθυνος για την εγκατάσταση των διορθωτικών πακέτων στα συστήματα ευθύνης του.

- **Τήρησης & Εγκατάστασης Λογισμικών**
  - ➢ Κατόπιν αιτήματος προς τους Διαχειριστές Δικτύου και Συστημάτων και κατόπιν της σύμφωνης γνώμης της Διοίκησης, σε ότι αφορά θέματα τήρησης και εγκατάστασης λογισμικών τρίτων, επιτρέπεται στους προγραμματιστές οι οποίοι ασχολούνται με την Ανάπτυξη Εφαρμογών. Η τήρηση και η εγκατάσταση διάφορων λογισμικών που είναι απαραίτητα εργαλεία για την διευκόλυνση της δουλειάς των προγραμματιστών αυτού του τμήματος, με μοναδική επιφύλαξη τη συμμόρφωσής τους με πολιτική ορθής και νόμιμης χρήσης του κάθε προγράμματος.

- **Αντίγραφα Ασφάλειας**
  - ➢ Θα πρέπει να λαμβάνονται αντίγραφα ασφάλειας για τον εξοπλισμό και τα δεδομένα της εταιρείας. Οι πληροφορίες για τις οποίες θα πρέπει να λαμβάνονται αντίγραφα ασφάλειας περιλαμβάνουν μελέτες, προσφορές, δεδομένα εργαζομένων, δεδομένα εφαρμογών, πηγαίος κώδικας λογισμικού, λειτουργικά συστήματα, αρχεία ρυθμίσεων εξοπλισμού, αρχεία καταγραφής (logs), δεδομένα επαλήθευσης χρηστών, οικονομικά δεδομένα.

- Ευθύνη για τη λήψη αντιγράφων ασφάλειας έχουν οι Διαχειριστές Δικτύου και Συστημάτων.
- Τα αντίγραφα ασφαλείας ταυτοποιούνται βάσει ημερομηνίας λήψης και ονόματός τους.
- Θα πρέπει να πραγματοποιούνται τακτικοί έλεγχοι ανάκτησης των πληροφοριών από τα αντίγραφα ασφάλειας, για να διαπιστωθεί η ακεραιότητα τους και η δυνατότητα ανάκτησης
- Υπεύθυνος για τη λήψη αντιγράφων ασφάλειας ενός συστήματος είναι οι Διαχειριστές Δικτύου και Συστημάτων που έχουν την ευθύνη διαχείρισης του συστήματος.
- Όταν ζητείται η ανάκτηση πληροφοριών από ένα αντίγραφο ασφάλειας, απαιτείται η έγκριση των Διαχειριστών Δικτύου και Συστημάτων.
- Τα αρχεία αντιγράφων ασφάλειας θα πρέπει να φέρουν ειδική σήμανση για να διευκολύνουν την ανεύρεση δεδομένων και να φυλάσσονται κατ' ελάχιστον και σε συστήματα τα οποία βρίσκονται σε χώρους οι οποίοι είναι διαχωρισμένοι από το σημείο όπου βρίσκονται τα αρχικά αντίγραφα ασφάλειας και φυλάσσονται από ανάλογα μέτρα ασφάλειας.
- Τα αντίγραφα ασφαλείας θα πρέπει να έχουν ελάχιστη ιστορικότητα διάρκειας πέντε (5) ημερών, εκτός και αν οι επιχειρησιακές ανάγκες της εταιρείας απαιτούν μεγαλύτερη διάρκεια τήρησης τους.
- Μετά τη λήξη της περιόδου τήρησης τους, τα αρχεία και τα αντίγραφα ασφαλείας θα καταστρέφονται σύμφωνα με την Οδηγία Καταστροφής Δεδομένων ή μέσω της διαδικασίας overwrite.

- **Παρακολούθηση και Καταγραφή**
  - Τα ενεργά μέρη των συστημάτων της εταιρείας δημιουργούν αρχεία καταγραφής τα οποία περιέχουν πλήθος δεδομένων σχετικά με τη λειτουργία, την κατάστασή τους, τις προσβάσεις χρηστών, τον φόρτο τους και τυχών σφάλματα που έχουν συμβεί. Αυτά τα αρχεία καταγραφής συλλέγονται από την εταιρεία σύμφωνα με τα όσα ορίζονται στη παρούσα πολιτική.

- Όλα τα αρχεία καταγραφής συγκεντρώνονται και αποθηκεύονται σε προστατευμένους χώρους, στους οποίους έχει πρόσβαση μόνο εξουσιοδοτημένο προσωπικό.
- Τα αρχεία καταγραφής θα πρέπει να κρατούνται κατ ’ελάχιστον για διάρκεια πέντε (5) ημερών, εκτός και αν οι επιχειρησιακές ανάγκες της εταιρείας απαιτούν μεγαλύτερη διάρκεια τήρησής τους.
- Τα αρχεία καταγραφής θα πρέπει να βρίσκονται σε μορφή άμεσα χρησιμοποιήσιμη από το προσωπικό, χωρίς να απαιτείται η χρήση πρόσθετου λογισμικού.
- Τα ρολόγια των συστημάτων θα πρέπει να είναι συγχρονισμένα προκειμένου να είναι εφικτός ο συσχετισμός αρχείων καταγραφής.
- Τα ενεργά στοιχεία της υποδομής θα πρέπει να παρακολουθούνται κατ’ ελάχιστον για το χρόνο που είναι ενεργά, τη διαθεσιμότητα τους και την κατάσταση τους.
- Στα αρχεία καταγραφής θα πρέπει να τηρούνται δεδομένα σχετικά με την πρόσβαση των χρηστών, λειτουργίες που απαιτούν πρόσβαση διαχειριστή, προσπάθειες για μη εξουσιοδοτημένη πρόσβαση, ειδοποιήσεις συστήματος, αλλαγές ή προσπάθειες τροποποίησης ρυθμίσεων ασφάλειας
- Κάθε εγγραφή στα αρχεία καταγραφής θα πρέπει κατ’ ελάχιστον να περιέχει:
  - Την ημέρα και την ώρα δημιουργίας της εγγραφής
  - Αύξοντα αριθμό της καταγραφής (όταν αυτή δημιουργείται με αυτόματο τρόπο)
  - Την ταυτότητα της οντότητας από την οποία προκλήθηκε η εγγραφή
  - Το είδος της εγγραφής
- Τα αρχεία καταγραφής να εξετάζονται σε περιοδική βάση (κατ’ ελάχιστον μία (1) φορά ανά μήνα), προκειμένου να εντοπιστούν περιστατικά δυσλειτουργιών ή περιστατικά ασφάλειας. Αυτοί οι έλεγχοι θα πρέπει να περιλαμβάνουν:
  - Επαλήθευση της ορθότητας και της μη τροποποίησης των αρχείων καταγραφής
  - Εξέταση των εγγραφών

- ❖ Διερεύνηση τυχών ειδοποιήσεων ή μη φυσιολογικών εγγραφών
- Οι ενέργειες που πραγματοποιούνται ως αποτέλεσμα της εξέτασης των αρχείων καταγραφής ακολουθούν τη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας.

- **Ασφάλεια Ηλεκτρονικών Υπηρεσιών**
  - Ιδιαίτερη μέριμνα τηρείται για τις υπηρεσίες που παρέχονται από την εταιρεία μέσω του site σε χρήστες εκτός του δικτύου της.
  - Η πληροφορία η οποία μεταδίδεται σε δημόσια δίκτυα πρέπει να προστατεύεται από παράνομη δραστηριότητα και να διασφαλίζεται η διεκπεραίωση κάθε συναλλαγής σύμφωνα με τις διαδικασίες που έχουν οριστεί.
  - Όλες οι συναλλαγές οι οποίες πραγματοποιούνται Online παρέχονται μέσα από υποδομές υψηλής διαθεσιμότητας, προκειμένου να διασφαλίζεται η επιχειρησιακή συνέχεια
  - Κατά τη μετάδοση εμπιστευτικών, προσωπικών ή ευαίσθητων δεδομένων εφαρμόζεται κρυπτογράφηση, με σκοπό την τήρηση της εμπιστευτικότητας των δεδομένων.
  - Στα πλαίσια των ηλεκτρονικών συναλλαγών, δεν αποστέλλονται και δεν κρατούνται από την εταιρεία στοιχεία κατόχων πιστωτικών/χρεωστικών καρτών των χρηστών και το σύνολο των πληρωμών πραγματοποιείται μέσα από μηχανισμούς και μέσα προστασίας που παρέχονται από το χρηματοπιστωτικό ίδρυμα με το οποίο συνεργάζεται η εταιρεία.
  - Οι εφαρμογές που αξιοποιούνται για την παροχή ηλεκτρονικών υπηρεσιών ενσωματώνουν μηχανισμούς ελέγχου που αποτρέπουν την λανθασμένη καταχώρηση δεδομένων από τους χρήστες και τυχόν λάθη που μπορεί να προκύψουν κατά τη μετάδοση πληροφοριών.
  - Για την αποφυγή σφαλμάτων που θα οδηγούσαν στην ασφάλεια της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας του πηγαίου κώδικα των εφαρμογών που αναπτύσσονται από την εταιρεία, οι εκδόσεις του πηγαίου κώδικα θα πρέπει να συγκεντρώνονται σε ένα κεντρικό σημείο (repository),

το οποίο θα πρέπει να είναι πάντα διαβαθμισμένο ως «Εμπιστευτικό» και να προστατεύεται με τα κατάλληλα μέτρα ασφάλειας.

- **Κρυπτογράφηση πληροφοριών**

Πίνακας 1 "Κρυπτογράφηση πληροφοριών εταιρίας"

RAID 1-mirroring 192,168,0,90,91 (Dell, pdc backup computer)	Εξασφαλίζει την αδιάλειπτη λειτουργία ακόμα και με 2 από τους 4 (50% of total capacity) δίσκους OFF
Encrypted partitions (Σε όλους Dell, backup computer)	Ασφάλεια δεδομένων και σε περίπτωση κλοπής
Primary Domain Controller (UCS - Linux)	Είσοδος μόνο σε εξουσιοδοτημένους χρήστες στο Domain της εταιρίας
File server – user quotas DELL	Ο κάθε χρήστης έχει δικό του χώρο για αποθήκευση αρχείων – όσο ορίζει με quotas ο διαχειριστής του Domain
Group Polices	δικαιώματα ορίζει ο administrator σε χρήστη (ή ομαδικά) και σε υπολογιστή (ή ομαδικά)
Backup Domain controller (RAID 1,encrypted partition)	Αναλαμβάνει την εργασία του PDC σε περίπτωση απώλειας του. Οι χρήστες δεν αντιλαμβάνονται τη μετάπτωση
Antivirus (DELL)	CLAMAV (Μελλοντικά ίσως περαστεί και στα 2 Linux και στο / partion)

Η εταιρία για διασφάλιση της διαρροής πληροφοριών εκούσιας ή ακούσιας σε τρίτους αλλά και για την ασφάλεια των δεδομένων της από μη εξουσιοδοτημένη πρόσβαση προχώρησε στην κρυπτογράφηση των δίσκων οι οποίοι τηρούν τα δεδομένα αυτά. Πιο συγκεκριμένα έγιναν και τηρούνται τα εξής :

- Δημιουργία και τήρηση εταιρικού Domain ώστε να υπάρχει μόνο εξουσιοδοτημένη πρόσβαση στους πόρους της εταιρίας και στα στοιχεία τα οποία τηρούνται σε αυτήν.

- Encrypted Partitions σε επίπεδο του File Server (User Quotas, Group Backup). Η κρυπτογράφηση έγινε κατά τη δημιουργία των δίσκων, ώστε τα δεδομένα τα οποία τηρούνται σε αυτούς τηρούνται κρυπτογραφημένα με σύνθετο κλειδί (32 χαρακτήρων). Το κλειδί τηρείται στα σχετικά αρχεία του ΥΔΑΠ, μαζί με άλλα στοιχεία όπως συνθηματικά χρηστών κ.λ.π.
- Αγορά και αναβάθμιση σε τελευταία έκδοση του OS στους σταθμούς εργασίας (Windows 10 Pro) έτσι ώστε να υπάρχει η δυνατότητα για Local Encrypted Disk Partitions στα οποία τηρούν οι χρήστες (Developers, Support) τον πηγαίο κώδικα ανάπτυξης, τα εκτελέσιμα των εφαρμογών και όχι μόνο. Με την τήρηση της κρυπτογράφησης και σε επίπεδο σταθμού εργασίας διασφαλίζεται –όσο αυτό είναι εφικτό- η διασφάλιση των δεδομένων από μη εξουσιοδοτημένη πρόσβαση και σε περίπτωση μεταφοράς σε περιβάλλον πέραν του εργασιακού χώρου (πχ πελάτη) αποτρέποντας και ανάστροφους μηχανισμούς όπως Reverse Engineering (*.exe to Source Code).

- **Επιχειρησιακή Συνέχεια (πλάνο)**

Για την διασφάλιση των πληροφοριών από κακόβουλο λογισμικό η εταιρία πραγματοποίησε την εξής δοκιμή. Δημιουργήθηκε ένα virtual machine το οποίο είναι πανομοιότυπο με σταθμό εργασίας. Ειδικότερα τα χαρακτηριστικά του μηχανήματος ήταν:

- Λειτουργικό Windows 10 pro
- Ram 2 GB
- HDD 40 GB
- Antivirus ESET όπως αυτό υπάρχει σε όλους τους σταθμούς εργασίας της εταιρείας
- Εγκατάσταση Oracle Client
- Εγκατάσταση του ERP
- Δοκιμαστική Λειτουργία

Στη συνέχεια έγινε απενεργοποίηση του Antivirus και φορτώθηκε ιός στον υπολογιστή (worm). Με την πάροδο του χρόνου έγινε αντιληπτό πως οι επιδόσεις του υπολογιστή άρχισαν να πέφτουν και γενικότερα υπήρχαν καθυστερήσεις

δικτύου και απόκρισης του υπολογιστή. Οι ενέργειες που ακολούθησαν ήταν οι εξής:

- Ενεργοποιήθηκε εκ νέου το Antivirus και έγινε full scan στον υπολογιστή
- Εντοπίστηκε το κακόβουλο λογισμικό
- Έγινε immune από το Antivirus και μπήκε σε καραντίνα
- Έγινε εκ νέου installation του ERP
- Έγινε επανεκκίνηση του υπολογιστή
- Ακολούθησε έλεγχος της λειτουργίας του.

Ο χρόνος από την αρχή της προσομοίωσης έως την αποκατάσταση ήταν κοντά στις τρεις (3) ώρες. Επίσης δε διαπιστώθηκε απώλεια δεδομένων (RDBMS) και λοιπών εγγράφων του υπολογιστή.

- Ολική επαναφορά – επαναλειτουργία της εταιρείας

  Για την ομαλή και απρόσκοπτη λειτουργία της εταιρείας έχει εκπονηθεί πλάνο για την αντιμετώπιση εκτάκτων περιπτώσεων-περιστατικών (π.χ. καταστροφή υποδομών, δικτύων, εξοπλισμού κ.λ.π.).

  Για τον λόγο αυτό η εταιρεία προμηθεύτηκε ένα Η/Υ (laptop) ο οποίος φυλάσσεται εκτός του χώρου των γραφείων της εταιρείας.

  Σε αυτόν υπολογιστή υπάρχουν φορτωμένα όλα τα απαραίτητα προγράμματα (software) έτσι ώστε άμεσα να υπάρχει η δυνατότητα επαναφοράς του τελευταίου back up (β1 κ.λ.π.) και να είναι εφικτή η υποστήριξη των πελατών της εταιρείας με το μικρότερο δυνατό downtime.

  Σε προσομοίωση που πραγματοποιήθηκε ο χρόνος αποκατάστασης (προσωρινής) ήταν της τάξεως των δύο (2) ωρών και περιλάμβανε τα εξής:

  - Μεταφορά του Η/Υ από τον χώρο φύλαξης (εκτός κτιρίου)
  - Εγκατάστασή του στον χώρο της εταιρείας
  - Restore DB
  - Σύνδεση ενός Η/Υ (Client) σε αυτόν
  - Δοκιμή

- **Διαχείριση Αποχώρησης Εργαζομένου**
  - Ο εταιρικός υπολογιστής παραδίδεται στον Υ.Δ.Α.Π.
  - Αλλαγή του κωδικού πρόσβασης του υπολογιστή
  - Backup του Δίσκου του υπολογιστή
  - Αλλαγή του κωδικού πρόσβασης στο mail account της εταιρείας
  - Backup των mail του εργαζόμενου
  - Redirect το mail σε global account
  - Το εταιρικό mail του εργαζόμενου καταργείται, αλλά διατηρείται η πρόσβαση σε αυτό από τον Υ.Δ.Α.Π. και την διοίκηση για εύλογο χρονικό διάστημα ανάλογα με την θέση του εργαζόμενου
  - Διαγραφή του λογαριασμού των Windows του εργαζόμενου
  - Ενημέρωση Πελατών για αποδέσμευση του εργαζόμενου
  - Ακύρωση εταιρικού τηλεφώνου, επαναφορά εργοστασιακών ρυθμίσεων
  - Οι προσβάσεις του εργαζόμενου καταργούνται ή αλλάζουν (αν υπάρχει αλλαγή θέσης) όπως προβλέπεται στην σχετική διαδικασία Δ14.
  - Τυχόν προσωπικά δεδομένα του εργαζόμενου που θα εντοπιστούν του παραδίδονται σε ηλεκτρονικό μέσω και διαγράφονται από τα μέσα της εταιρείας.

- **Χρησιμοποιούμενα Έντυπα και αρχειοθέτηση**

Α/Α	ΑΡΧΕΙΟ	ΕΠΙΣΥΝΑΠΤΟΜΕΝΑ		ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ ΑΡΧΕΙΟΥ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ
		ΕΝΤΥΠΟ	ΚΩΔΙΚΟΣ		

2.2 Πολιτική αποδεκτής χρήσης

Ο σκοπός αυτής της πολιτικής είναι να καθοριστεί ο τρόπος με τον οποίο οι χρήστες θα πρέπει να αξιοποιούν και να χρησιμοποιούν τους υπολογιστικούς και πληροφοριακούς πόρους της εταιρείας, προκειμένου η χρήση και η αξιοποίηση τους να είναι σύμφωνη με τις επιχειρηματικές, νομικές και κανονιστικές απαιτήσεις, όπως ορίζονται στις πολιτικές της εταιρείας.

Τα δίκτυα (Internet / Intranet / Extranet), αλλά και τα σχετιζόμενα με αυτά συστήματα, συμπεριλαμβανομένων του υπολογιστικού εξοπλισμού (Η/Υ), του λογισμικού, των λειτουργικών συστημάτων, των μέσων αποθήκευσης, των λογαριασμών παροχής πρόσβασης, του ηλεκτρονικού ταχυδρομείου και όλων των υποδομών της εταιρίας είναι ιδιοκτησία της. Τα συστήματα αυτά προορίζονται για την εξυπηρέτηση των συμφερόντων της εταιρείας, καθώς και των εργαζομένων του κατά τη διάρκεια της κανονικής λειτουργίας.

Η αποτελεσματική ασφάλεια είναι μια ομαδική προσπάθεια και απαιτεί τη συμμετοχή και υποστήριξη κάθε εργαζόμενου. Είναι η ευθύνη κάθε χρήστη οποιουδήποτε υπολογιστικού και πληροφοριακού πόρου της εταιρίας να γνωρίζει αυτές τις οδηγίες, και να ασκεί τις δραστηριότητές τους αναλόγως. Η πολιτική αυτή εφαρμόζεται σε όλη την εταιρεία και αφορά όλα τα στελέχη και το προσωπικό της εταιρείας.

2.2.1 Υπευθυνότητες

- Η Διοίκηση έχει την ευθύνη παροχής στους χρήστες των υπολογιστικών και πληροφοριακών συστημάτων της εταιρείας, των μέσων που απαιτούνται για τη τήρηση των όσων ορίζονται στη παρούσα πολιτική
- Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών, έχει την ευθύνη ενημέρωσης των χρηστών των πληροφοριακών και υπολογιστικών συστημάτων της εταιρείας για το περιεχόμενο και τη χρήση της παρούσας πολιτικής, αλλά και τη διαρκή επικαιροποίηση και βελτίωσή της
- Όλοι οι χρήστες των πληροφοριακών και υπολογιστικών πόρων, έχουν την ευθύνη τήρησης των όσων ορίζονται στη παρούσα πολιτική κατά τη διεκπεραίωση των καθημερινών του καθηκόντων.

2.2.2 Περιγραφή

- **Γενικές οδηγίες**
  - Η Διοίκηση της εταιρείας επιθυμεί να παρέχει το μέγιστο δυνατό επίπεδο προστασίας της ιδιωτικής ζωής, αλλά οι χρήστες πρέπει να γνωρίζουν ότι τα δεδομένα που δημιουργούν στα εταιρικά συστήματα παραμένουν ιδιοκτησία της εταιρίας και ότι αρχεία προσωπικού χαρακτήρα δε θα πρέπει να τηρούνται εντός αυτού. Λόγω της ανάγκης για την προστασία του δικτύου, η διοίκηση δεν μπορεί να εγγυηθεί το απόρρητο των πληροφοριών

που είναι αποθηκευμένες σε οποιαδήποτε συσκευή ή μέσο μετάδοσης το οποίο ανήκει στην εταιρία.

- Οι χρήστες του υπολογιστικού και πληροφοριακού συστήματος της εταιρίας είναι υπεύθυνοι για την άσκηση ορθής κρίσης σχετικά με το εύλογο της προσωπικής χρήσης. Οι εργαζόμενοι θα πρέπει να καθοδηγούνται από τη νομοθεσία για τη προσωπική χρήση, και αν υπάρχει κάποια αβεβαιότητα, οι εργαζόμενοι θα πρέπει να συμβουλεύονται προϊστάμενο ή διευθυντή τους.
- Για την ασφάλεια και για λόγους συντήρησης δικτύου, εξουσιοδοτημένο προσωπικού της εταιρείας ενδέχεται να παρακολουθεί τον εξοπλισμό, τα συστήματα και τη μετάδοση των πληροφοριών στο δίκτυο, ανά πάσα στιγμή.
- Η εταιρεία διατηρεί το δικαίωμα να επιθεωρεί το δίκτυο και τα συστήματα ελέγχου σε περιοδική βάση για να εξασφαλιστεί η συμμόρφωση με αυτή την πολιτική
- Στις εγκαταστάσεις ασφαλείας οι εργαζόμενοι οφείλουν να τηρούν τάξη στις θέσεις εργασίας τους και να μην αφήνουν στην επιφάνεια αυτών, έγγραφα και εξοπλισμό, που δεν χρησιμοποιούν.
- Στα υπολογιστικά συστήματα, που περιλαμβάνονται στο σύστημα ασφάλειας πληροφοριών, οι χρήστες οφείλουν να τηρούν τάξη στην αρχειοθέτηση των δεδομένων τους και να κρατούν καθαρό desktop, ώστε να διευκολύνεται η χρήση.

- **Ασφάλεια και ιδιόκτητες πληροφορίες**
  - Οι χρήστες του υπολογιστικού και πληροφοριακού συστήματος της εταιρείας θα πρέπει να διαβαθμίζουν και να χρησιμοποιούν τις πληροφορίες (ψηφιακές ή όχι), σύμφωνα με την Οδηγία Διαβάθμισης Δεδομένων.
  - Οι χρήστες του υπολογιστικού και πληροφοριακού συστήματος της εταιρείας θα πρέπει να λαμβάνουν όλα τα αναγκαία μέτρα για την αποτροπή μη εξουσιοδοτημένης πρόσβασης στις πληροφορίες και τους πόρους του συστήματος.
  - Οι χρήστες του υπολογιστικού και πληροφοριακού συστήματος θα πρέπει να τηρούν τους κωδικούς πρόσβασης μυστικούς και να μη τους μοιράζονται.

Οι εξουσιοδοτημένοι χρήστες είναι υπεύθυνοι για την τήρηση της εμπιστευτικότητας των κωδικών πρόσβασης και των λογαριασμών τους

- Οι κωδικοί πρόσβασης στα συστήματα θα πρέπει να αλλάζονται ανά τακτά διαστήματα, σύμφωνα με ότι ορίζεται στην Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων.

- **Χρήση Εξοπλισμού**
  - Όλοι οι υπολογιστές, φορητοί υπολογιστές και σταθμοί εργασίας, θα πρέπει να ασφαλίζονται με ένα προστατευμένο με κωδικό screensaver με τη δυνατότητα αυτόματης ενεργοποίησης που ορίζεται στα 30 λεπτά ή λιγότερο, ή με logging-off.
  - Οι Η/Υ και οι φορητοί Η/Υ που χρησιμοποιούνται από τους χρήστες των πληροφοριακών συστημάτων και είναι συνδεδεμένοι με τις δικτυακές υποδομές (Internet/Intranet/Extranet), πρέπει να έχουν εγκατεστημένο, ενημερωμένο και συνεχώς ενεργό εγκεκριμένο λογισμικό ανίχνευσης ιών.
  - Οι χρήστες πρέπει να είναι ιδιαίτερα προσεκτικοί όταν ανοίγουν συνημμένα e-mail που έλαβαν από άγνωστους αποστολείς, που ενδέχεται να περιέχουν ιούς, e-mailbombs, ή Trojanhorse code.

- **Συστημικές και Δικτυακές Δραστηριότητες**

Οι ακόλουθες δραστηριότητες, σε γενικές γραμμές, απαγορεύονται. Οι χρήστες μπορούν να εξαιρεθούν από τους περιορισμούς αυτούς κατά τη διάρκεια της δουλειάς τους. Δεν επιτρέπεται σε καμία περίπτωση χρήστες της εταιρίας να συμμετέχουν σε οποιαδήποτε δραστηριότητα, η οποία είναι παράνομη σύμφωνα με το ελληνικό ή το διεθνές δίκαιο, ενώ χρησιμοποιεί πόρους του δικτύου της εταιρείας. Οι ακόλουθες δραστηριότητες απαγορεύονται αυστηρά, χωρίς εξαιρέσεις:

- Η παραβίαση των δικαιωμάτων οποιουδήποτε προσώπου της εταιρείας που προστατεύονται από πνευματικά δικαιώματα, εμπορικά μυστικά, διπλώματα ευρεσιτεχνίας ή άλλα δικαιώματα πνευματικής ιδιοκτησίας, ή παρόμοιων νόμων ή κανονισμών, συμπεριλαμβανομένων της εγκατάστασης ή τη διανομής της «πειρατείας» ή άλλων προϊόντων λογισμικού που δεν έχουν κατάλληλη άδεια για χρήση από την εταιρία.

- Η μη εξουσιοδοτημένη αντιγραφή υλικού το οποίο προστατεύεται από πνευματικά δικαιώματα, συμπεριλαμβανομένων της ψηφιοποίησης και της διανομής φωτογραφιών από περιοδικά, βιβλία ή άλλες πηγές πνευματικών δικαιωμάτων, πνευματικά δικαιώματα της μουσικής.
- Η εγκατάσταση οποιουδήποτε λογισμικού για τα οποία η εταιρία ή ο τελικός χρήστης δεν έχει ενεργή άδεια.
- Η εισαγωγή κακόβουλων προγραμμάτων στο δίκτυο ή στους διακομιστές (π.χ. ιούς, worms, δούρειους ίππους, e -mail bombs, κ.λ.π.)
- Η αποκάλυψη του κωδικού πρόσβασης του λογαριασμού σας σε τρίτους ή η χρήση του λογαριασμού πρόσβασης από τους. Αυτό περιλαμβάνει και την οικογένεια, όταν η εργασία γίνεται στο σπίτι.
- Η αξιοποίηση πόρων της εταιρείας για την ενεργό συμμετοχή στη προμήθεια ή μετάδοση υλικού που παραβαίνει τη νομοθεσία περί σεξουαλικής παρενόχλησης ή τη νομοθεσία που σχετίζεται με τη συμπεριφορά στο χώρο εργασίας.
- Η πραγματοποίηση κακόβουλων προσφορών προϊόντων, ειδών ή υπηρεσιών αξιοποιώντας οποιονδήποτε πόρο της εταιρίας.
- Η παραβίαση της ασφάλειας ή η διακοπή της επικοινωνίας του δικτύου. Οι παραβιάσεις της ασφάλειας περιλαμβάνουν πρόσβαση στα δεδομένα των οποίων ο χρήστης δεν είναι ο προοριζόμενος παραλήπτης ή η πρόσβαση σε διακομιστή ή λογαριασμό χρήστη στα οποία ο χρήστης δεν επιτρέπεται ρητά να έχει πρόσβαση , εκτός και αν τα καθήκοντα αυτά εμπίπτουν στο πεδίο εφαρμογής των τακτικών καθηκόντων του.
- Η σάρωση δικτυακών πόρων (port scan / network scan) απαγορεύεται ρητά εκτός αν έχουν δοθεί εντολές από τον Υ.Δ.Α.Π. ή από τους Διαχειριστές Δικτύου και Συστημάτων.
- Η εκτέλεση κάθε μορφής παρακολούθησης ή παρέμβασης στις δικτυακές της εταιρίας εκτός αν αυτή η δραστηριότητα είναι ένα μέρος της κανονικής εργασίας / καθήκον του εργαζόμενου.
- Η παράκαμψη της διαδικασίας αυθεντικοποίησης / ταυτοποίησης ή των μέτρων ασφάλειας οποιουδήποτε υπολογιστή , δικτύου ή λογαριασμού.
- Η παρεμβολή ή η άρνηση παροχής υπηρεσιών σε οποιοδήποτε χρήστη.

- Η χρήση οποιουδήποτε προγράμματος / script / εντολής εκτός αυτών που έχουν εγκριθεί από τον admistrator., ή η αποστολή μηνυμάτων κάθε είδους, με την πρόθεση τη παρεμβολή ή την απενεργοποίηση του τερματικού ενός χρήστη τοπικά ή μέσω του Internet / Intranet / Extranet.(SMTP Card for the UPS Automated Script for shutting down any network attached devices p.e. Laptops/ Terminals/ Work Stations)
- Η παροχή πληροφοριών σχετικά με τους χρήστες της εταιρίας σε φορείς εκτός εταιρείας.

- **E-mail και Δραστηριότητες Επικοινωνίας**

Οι ακόλουθες δραστηριότητες, απαγορεύονται. Δεν επιτρέπεται σε καμία περίπτωση χρήστης της εταιρίας να συμμετέχει σε οποιαδήποτε δραστηριότητα η οποία είναι παράνομη σύμφωνα με το ελληνικό ή το διεθνές δίκαιο, ενώ χρησιμοποιεί πόρους της εταιρείας

- Η αποστολή και η χρήση αυτόκλητων μηνυμάτων ηλεκτρονικού ταχυδρομείου, συμπεριλαμβανομένων των εξόδων αποστολής «ανεπιθύμητης αλληλογραφίας» ή άλλου διαφημιστικού υλικού σε φυσικά πρόσωπα που δεν έχουν ζητήσει το εν λόγω υλικό (spam e-mail).
- Η πραγματοποίηση οποιασδήποτε μορφής παρενόχληση μέσω ηλεκτρονικού ταχυδρομείου, τηλεφώνου ή τηλεειδοποίησης, ανεξάρτητα αν αυτή η παρενόχληση είναι λεκτική ή σχετίζεται με τη συχνότητα ή το μέγεθος των μηνυμάτων ή της επικοινωνίας.
- Η μη εξουσιοδοτημένη χρήση των πληροφοριών ηλεκτρονικού ταχυδρομείου.
- Η συγκέντρωση μηνυμάτων ή διευθύνσεων ηλεκτρονικό για οποιαδήποτε άλλη ηλεκτρονική διεύθυνση, με την πρόθεση τη παρενόχληση ή τη συλλογή απαντήσεων.
- Κάθε σχόλιο από τους υπαλλήλους της εταιρίας μέσω διεύθυνσης ηλεκτρονικού ταχυδρομείου σε ομάδες συζήτησης θα πρέπει να συνοδεύεται από δήλωση ότι οι απόψεις που εκφράζονται είναι δικές τους και όχι απαραίτητα εκείνες της εταιρίας εκτός αν αυτές οι γνώμες εμπίπτουν στο αντικείμενο εργασίας τους.

- **Χρησιμοποιούμενα Έντυπα και αρχειοθέτηση**

Α/Α	ΑΡΧΕΙΟ	ΕΠΙΣΥΝΑΠΤΟΜΕΝΑ		ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ ΑΡΧΕΙΟΥ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ
		ΕΝΤΥΠΟ	ΚΩΔΙΚΟΣ		

2.3 Πολιτική ελέγχου πρόσβασης

Σκοπός της παρούσης Πολιτικής είναι να ορίσει τον τρόπο με τον οποίο η εταιρεία θα ελέγχει την πρόσβαση σε πληροφορίες, υποδομές, χώρους και διαδικασίες, ώστε να εξασφαλίζεται το αποδεκτό επίπεδο εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας των πληροφοριακών συστημάτων. Η παρούσα πολιτική στόχο έχει να διασφαλίσει ότι μόνο εξουσιοδοτημένοι χρήστες αποκτούν πρόσβαση σε πόρους της εταιρείας και το πεδίο εφαρμογής της περιλαμβάνει όλους τους χρήστες των πληροφοριακών συστημάτων, συμπεριλαμβανομένων των εξωτερικών συνεργατών και τρίτων μερών τα οποία αποκτούν πρόσβαση σε χώρους, συστήματα ή πληροφορίες της. Η πολιτική αυτή εφαρμόζεται σε όλη την εταιρεία και αφορά όλα τα στελέχη και το προσωπικό της εταιρείας.

2.3.1 Υπευθυνότητες

Οι Διαχειριστές Δικτύου και Συστημάτων, είναι υπεύθυνοι για την πραγματοποίηση όλων των ενεργειών, τεχνικών ή οργανωτικών, που απαιτούνται για την τήρηση των όσων ορίζονται στη παρούσα πολιτική. Ο Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών – στη συνέχεια θα αναγράφεται ως Υ.Δ.Α.Π., είναι υπεύθυνος για τη διασφάλιση της τήρησης των όσων ορίζονται στην παρούσα πολιτική, αλλά και για την επικαιροποίηση, διόρθωση ή συντήρησή της.

2.3.2 Περιγραφή

- **Έλεγχος πρόσβασης**
  - Η πρόσβαση στους πληροφοριακούς και υπολογιστικούς πόρους της εταιρίας θα παρέχεται κατά τρόπο που θα διασφαλίζει ότι κάθε χρήστης ή ομάδα χρηστών έχει πρόσβαση σε συγκεκριμένους πόρους.

- Κάθε πληροφοριακός και υπολογιστικός πόρος της εταιρείας είναι μέρος ενός ευρύτερου συστήματος. Οι Διαχειριστές Δικτύου και Συστημάτων είναι υπεύθυνοι να παρέχουν το απαραίτητο επίπεδο πρόσβασης στους πόρους που ανήκουν στο εκάστοτε σύστημα.
- Ο Υ.Δ.Α.Π. είναι υπεύθυνος περιοδικά να εξετάζει την πρόσβαση που έχει παρασχεθεί σε πόρους των συστημάτων, προκειμένου να διασφαλίζει ότι η πρόσβαση έχει δοθεί σύμφωνα με τις επιχειρησιακές απαιτήσεις και τα όσα ορίζονται στη παρούσα πολιτική και δύναται να αιτηθεί την αφαίρεση δικαιωμάτων πρόσβασης που έχουν παρασχεθεί σε χρήστες ή ομάδες χρηστών.
- Τα δικαιώματα πρόσβασης χρηστών και ομάδων χρηστών ελέγχονται μία φορά ανά έτος και μετά από κάθε σχετική οργανωσιακή αλλαγή, όπως η μετακίνηση στην ιεραρχία ή ο τερματισμός της συνεργασίας ή της εργασίας ενός χρήστη.
- Τα δικαιώματα πρόσβασης σε συστήματα που έχουν διαβαθμιστεί ως εμπιστευτικά θα πρέπει να εξετάζονται δύο φορές ετησίως.
- Κάθε χρήστης έχει μοναδικό λογαριασμό χρήστη στα συστήματα της εταιρείας, μέσω του οποίου πραγματοποιεί το σύνολο των διαδικασιών. Ταυτοχρόνως πρέπει να γίνεται σε τεχνικό επίπεδο συγκεκριμένη εκχώρηση δικαιωμάτων/εξουσιοδοτήσεων σε κάθε χρήστη (εργαζόμενοι, συνεργάτες, ανάδοχοι, εξωτερικοί χρήστες κ.α.).
- Η προσθήκη, μεταβολή και διαγραφή λογαριασμών χρηστών θα πρέπει να πραγματοποιείται μέσω της διαδικασίας παροχής πρόσβασης χρηστών.
- Πρέπει να υπάρχουν κατάλληλοι μηχανισμοί ώστε να απαγορεύεται η πρόσβαση σε έναν εξουσιοδοτημένο χρήστη, μετά από ένα πλήθος επαναλαμβανομένων αποτυχημένων αιτήσεων πρόσβασης (για παράδειγμα, υποβολή λανθασμένων συνθηματικών).
- Όταν ένας σταθμός εργασίας είναι αδρανής για μεγάλο χρονικό διάστημα (μέγιστο όριο τα 30 λεπτά), ο χρήστης θα πρέπει να αποσυνδέεται αυτόματα ή να ενεργοποιείται η προφύλαξη οθόνης και να απαιτείται η επανάληψη της αυθεντικοποίησης του χρήστη.

- Στα δεδομένα τα οποία χρησιμοποιούνται για δοκιμές κατά την ανάπτυξη προγραμμάτων ή παροχή υπηρεσιών θα πρέπει να εφαρμόζονται τα ίδια μέτρα ελέγχου πρόσβασης, είτε να τροποποιούνται με κατάλληλους μηχανισμούς (data masking) ώστε να καθίστανται μη αναγνωρίσιμα ή αξιοποιήσιμα σε μη εξουσιοδοτημένους χρήστες
- Η πρόσβαση σε όλες της εκδόσεις του πηγαίου κώδικας (source code) των εφαρμογών της εταιρίας θα πρέπει να ελέγχεται, τόσο κεντρικά, όσο και στα σημεία στα οποία αυτός αναπτύσσεται.

- **Συνθηματικά Πρόσβασης**

Τα συνθηματικά χρηστών θα πρέπει να έχουν κατ' ελάχιστον τα παρακάτω χαρακτηριστικά

- Ελάχιστο μήκος χαρακτήρων: 8 χαρακτήρες
- Συνδυασμός τουλάχιστον δύο (2) από τους παρακάτω τύπους χαρακτήρες:
  - Πεζοί χαρακτήρες (a-z)
  - Κεφαλαίοι χαρακτήρες (A-Z)
  - Αριθμοί (1-9)
  - Ειδικοί χαρακτήρες, όπως οι: !@#$%^&*(){}[]
- Ίδια πολιτική ακολουθείται και στα εταιρικά e-mail accounts της μορφής username@etairia.gr και καθορίζεται από τους διαχειριστές συστημάτων και δικτύου από την πλατφόρμα διαχείρισης των λογαριασμών του παρόχου.
- Οι χρήστες πρέπει να υποχρεώνονται να αλλάζουν οι ίδιοι το (προκαθορισμένο) συνθηματικό που τους ανατίθεται εξαρχής.
- Η μέγιστη διάρκεια ζωής ενός συνθηματικού είναι 90 ημέρες.
- Τα συνθηματικά πρόσβασης χρηστών δεν πρέπει να είναι κάπου καταγεγραμμένα στην πραγματική τους μορφή (ούτε σε φυσικό ούτε σε ηλεκτρονικό αρχείο).
- Εάν τα συνθηματικά διατηρούνται ηλεκτρονικά στο πλαίσιο της διαδικασίας ταυτοποίησης-αυθεντικοποίησης των χρηστών, τότε πρέπει να είναι σε μη αναγνώσιμη μορφή από την οποία δεν πρέπει να είναι εφικτή η ανάκτηση της αρχικής τους μορφής.

- **Αρχεία καταγραφής (logfiles)**

  - Στα συστήματα, θα πρέπει να καταγράφονται ενέργειες που πραγματοποιούνται με διαχειριστικά δικαιώματα, προσπάθειες πρόσβασης, καθώς συμβάντα ασφαλείας που επισημαίνονται από τα συστήματα.
  - Στα αρχεία καταγραφής δύναται να έχει πρόσβαση ο Υ.Δ.Α.Π. και η Ομάδα Ασφάλειας και Ποιότητας.
  - Πρέπει να τηρούνται στοιχεία που αφορούν τις προσπάθειες μη εξουσιοδοτημένης πρόσβασης και τις αλλαγές στην παραμετροποίηση εφαρμογών και συστημάτων, τον προκαθορισμό κρίσιμων γεγονότων (events), η καταγραφή των οποίων θα επιβλέπεται από τον Υ.Δ.Α.Π. και την Ομάδα Ποιότητας και Ασφάλειας και γενικότερα κάθε ενέργεια η οποία μπορεί να υποδηλώνει διενέργεια επίθεσης, όπως προσπάθειες καταγραφής των προσφερόμενων υπηρεσιών του συστήματος (portscanning).

- **Φυσική Πρόσβαση**

  - Πρέπει να υπάρχουν τα κατάλληλα μέτρα ελέγχου φυσικής πρόσβασης στους χώρους όπου βρίσκεται ο φυσικός εξοπλισμός (συμπεριλαμβανομένης τηλεπικοινωνιακής και δικτυακής καλωδίωσης) που υποστηρίζει τα πληροφοριακά συστήματα και την επεξεργασία προσωπικών δεδομένων.
  - Η πρόσβαση σε αυτούς τους χώρους επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό και θα παρέχεται με την έγκριση των Υ.Δ.Α.Π., της Ομάδας Ποιότητας και Ασφάλειας καθώς και των Διαχειριστών Δικτύου και Συστημάτων.
  - Τα δικαιώματα πρόσβασης περιγράφονται στο πίνακα Employees Access Control.

- **Χρησιμοποιούμενα Έντυπα και αρχειοθέτηση**

Α/Α	ΑΡΧΕΙΟ	ΕΠΙΣΥΝΑΠΤΟΜΕΝΑ		ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ ΑΡΧΕΙΟΥ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ
		ΕΝΤΥΠΟ	ΚΩΔΙΚΟΣ		

2.4 Πολιτική ελέγχου τρίτων μερών

Σκοπός της παρούσας πολιτικής είναι να ελαττώσει τους κινδύνους ασφάλειας πληροφοριών που σχετίζονται με δραστηριότητες που πραγματοποιούνται από τρίτα μέρη, εκτός της εταιρίας. Τέτοιοι κίνδυνοι μπορεί να προκύψουν από την παροχή μη εξουσιοδοτημένης πρόσβασης, την απώλεια της εμπιστευτικότητας πληροφοριών και δεδομένων της εταιρείας, την απώλεια προστασίας της πνευματικής ιδιοκτησίας ή οποιαδήποτε ενέργεια ή αμέλεια τρίτων μερών που θα μπορούσε να προκαλέσει βλάβη στην εμπιστευτικότητα, ακεραιότητα ή διαθεσιμότητα των πόρων της εταιρείας. Η πολιτική αυτή εφαρμόζεται σε όλη την εταιρεία και αφορά όλα τα στελέχη και το προσωπικό της εταιρείας.

2.4.1 Υπευθυνότητες

- Η Διοίκηση, όσον αφορά τον καθορισμό της Διαδικασίας και την αποτίμηση της αποτελεσματικότητας της καθώς και όλο το προσωπικό της εταιρείας κατά τη διεκπεραίωση των καθημερινών του καθηκόντων
- Ο Υπεύθυνος Δ.Α.Π. και οι είναι υπεύθυνος για την αξιολόγηση και τη διαχείριση των εμπορικών κινδύνων και των κινδύνων ασφαλείας που συνδέονται με Τρίτα Μέρη
- Οι Διαχειριστές Δικτύου και Συστημάτων είναι υπεύθυνοι για τους κινδύνους ασφαλείας που συνδέονται με Τρίτα Μέρη.

2.4.2 Περιγραφή

- **Επιλογή ενός τρίτου παρόχου.** Τα κριτήρια για την επιλογή ενός παρόχου θα πρέπει να καθορίζονται και να τεκμηριώνονται λαμβάνοντας υπόψη κατ' ελάχιστον τους παρακάτω παράγοντες:
  - φήμη και την ιστορία της εταιρείας
  - ποιότητα των παρεχόμενων υπηρεσιών προς άλλους πελάτες
  - τον αριθμό και τα προσόντα του προσωπικού και των διευθυντών
  - χρηματοπιστωτική σταθερότητα της εταιρίας και του εμπορικού ρεκόρ
  - ποσοστά διατήρησης των εργαζομένων της εταιρίας

- διασφάλισης της ποιότητας και πρότυπα διαχείρισης της ασφάλειας που ακολουθούνται από την εταιρεία (π.χ. επικυρωμένα σύμφωνα με τα πρότυπα ISO9001 και ISO/IEC27001).

- **Αξιολόγηση κινδύνων.** Η Διοίκηση ορίζει έναν Υπεύθυνο Έργου για κάθε επιχειρηματική λειτουργία / διαδικασία που αναθέτει σε εξωτερικούς συνεργάτες. Ο Υπεύθυνος Έργου, με τη βοήθεια του Υ.Δ.Α.Π. αξιολογεί τους κινδύνους και τις απειλές για την ασφάλεια πληροφοριών, πριν από τη λειτουργία / διαδικασία που έχει ανατεθεί σε εξωτερικούς συνεργάτες. Αυτή η αποτίμηση επικινδυνότητας, λαμβάνει υπόψη της:
  - τη φυσική πρόσβαση σε περιουσιακά στοιχεία και εγκαταστάσεις της εταιρείας που απαιτούνται από τον πάροχο έτσι ώστε να εκπληρώσει τη σύμβαση
  - την ευαισθησία, τον όγκο και την αξία των πληροφοριών και των πόρων τα οποία ενδέχεται να επηρεαστούν από τις εργασίες των Τρίτων Μερών
  - τους εμπορικούς κινδύνους, όπως τη πιθανότητα ο πάροχος να μην επιτελέσει τις λειτουργίες που του έχουν ανατεθεί με τα αναμενόμενα αποτελέσματα

Το αποτέλεσμα της αξιολόγησης κινδύνων πρέπει να διαβιβάζεται στον Υ.Δ.Α.Π., ο οποίος ενημερώνει την Διοίκηση για τους κινδύνους που σχετίζονται με το έργο.

- **Εξέταση επικινδυνότητας εξωτερικής ανάθεσης.** Η Διοίκηση αποφασίζει αν η εταιρεία επωφελείται από την εξωτερική ανάθεση της λειτουργίας στον πάροχο, λαμβάνοντας υπόψη τόσο τις εμπορικές όσο και τις πληροφοριακές πτυχές της εκτίμησης επικινδυνότητας. Εάν οι κίνδυνοι που εμπλέκονται εκτιμηθούν ως υψηλοί και τα οφέλη οριακά, η Διοίκηση έχει τη δυνατότητα είτε να ζητήσει την εξέταση εναλλακτικών τρίτων μερών, είτε να αναθέσει το έργο σε προσωπικό της εταιρίας.
- **Συμφωνίες εμπιστευτικότητας**.
  - Πρέπει να υπάρχει σύμβαση μεταξύ εταιρίας και τρίτων μερών, στην οποία θα καθορίζεται ο σκοπός και το είδος των ανταλλασσόμενων πληροφοριών.

- Η σύμβαση πρέπει να καθορίζει σαφώς τις ευθύνες του κάθε μέρους προς το άλλο με τον καθορισμό των μερών της σύμβασης , ημερομηνία έναρξης ισχύος , λειτουργίες ή υπηρεσίες που παρέχονται (π.χ. καθορισμένα επίπεδα υπηρεσιών), οι υποχρεώσεις, οι περιορισμοί σχετικά με τη χρήση των υπεργολάβων και των άλλων εμπορικών / νομικά θέματα σε κάθε σύμβαση .
- Ανάλογα με τα αποτελέσματα της αξιολόγησης κινδύνων , πρόσθετοι έλεγχοι είναι δυνατό να ενσωματωθούν ή να αναφέρονται στο πλαίσιο της σύμβασης , οι οποίοι σχετίζονται με:
  - Νομοθετικές, κανονιστικές και άλλες υποχρεώσεις τρίτων μερών, όπως η προστασία των δεδομένων / νόμων περί ιδιωτικής ζωής , ξέπλυμα χρήματος κ.λπ.
  - Τον έλεγχο ιστορικού εργαζομένων ή τρίτων που εργάζονται για τη σύμβαση.
  - Την πρόσβαση που παρέχεται στους εργαζομένους τρίτων μερών, συμπεριλαμβανομένων των φυσικών και λογικών ελέγχων πρόσβασης.
  - Περιστατικά ασφάλειας πληροφοριών και διαδικασίες διαχείρισης τους.
  - Την επιστροφή ή καταστροφή όλων των πληροφοριακών ή άλλον πόρων που ελήφθησαν από τον τρίτο πάροχο μετά την ολοκλήρωση της ανατιθέμενης δραστηριότητας ή κάθε φορά που ένας πόρος δεν απαιτείται πια για την εξωτερική ανάθεση δραστηριοτήτων.
  - Διαχείριση και προστασία των πνευματικών δικαιωμάτων και των διπλωμάτων ευρεσιτεχνίας.
  - Τα μέτρα πρόληψης για την αποφυγή διάδοσης malware, αποστολής spam ή άλλων τεχνικών κινδύνων.
  - Τη διαχείριση και πραγματοποίησης αλλαγών, συμπεριλαμβανομένης της αποτίμησης και διαχείρισης ευπαθειών, πριν την εφαρμογή των αλλαγών στα παραγωγικά συστήματα του Ιδρύματος.
- Εάν οι πληροφορίες που ανταλλάσσονται είναι εμπιστευτικές, μια δεσμευτική συμφωνία εμπιστευτικότητας πρέπει να γίνεται μεταξύ της εταιρίας και εξωτερικών συνεργατών, είτε ως μέρος της ίδιας της σύμβασης,

είτε ως ξεχωριστή συμφωνία μη-αποκάλυψης (Non-Disclosure Aggreement).

- Οι απαιτήσεις ασφάλειας πληροφοριών διαβαθμίζονται και ελέγχονται σύμφωνα με τις πολιτικές ασφάλειας πληροφοριών της εταιρίας.
- Οι πληροφορίες της εταιρίας που λαμβάνονται από τρίτα μέρη τα οποία δεσμεύονται σύμβαση ή συμφωνία εμπιστευτικότητας θα πρέπει να είναι αναγνωρίσιμες και να προστατεύονται με τα κατάλληλα μέτρα προστασίας.
- Μετά τη λήξη της σύμβασης, οι απαιτήσεις εμπιστευτικότητας θα πρέπει να επανεξεταστούν για να καθοριστεί κατά πόσον η εμπιστευτικότητα πρέπει να επεκταθεί πέρα από τη διορία της σύμβασης.
- Όλες οι συμβάσεις θα πρέπει να ελέγχονται ως προς την νομική τους ορθότητα, την ακρίβεια του περιεχομένου, της γλώσσας και της παρουσίασης τους.
- Η εταιρεία διατηρεί το δικαίωμα ελέγχου των προσβάσεων και της χρήσης των εγκαταστάσεων της εταιρείας, όπως δίκτυα, συστήματα κ.λπ., καθώς και τον έλεγχο της συμμόρφωσης του παρόχου με τη σύμβαση. Οι έλεγχοι αυτοί δύνανται να πραγματοποιούνται από προσωπικό της εταιρίας ή να χρησιμοποιείται ένας αμοιβαία αποδεκτός, ανεξάρτητος εξωτερικός ελεγκτής για το σκοπό αυτό.

- **Προσωπικό τρίτων μερών.**

- Οι ανάδοχοι εργαζόμενοι και σύμβουλοι που εργάζονται για λογαριασμό της εταιρίας πρέπει να υποβάλλονται σε ελέγχους του ιστορικού ισοδύναμους με εκείνους που εκτελούνται στους εργαζόμενους της εταιρίας. Αυτός ο έλεγχος λαμβάνει υπόψη το επίπεδο της εμπιστοσύνης και την ευθύνη που σχετίζεται με τη θέση και (όπου επιτρέπεται από την τοπική νομοθεσία):
  - Η απόδειξη της ταυτότητας του προσώπου (π.χ. διαβατήριο)
  - Η απόδειξη των ακαδημαϊκών προσόντων τους (π.χ. πιστοποιητικά)
  - Η απόδειξη της επαγγελματικής τους εμπειρίας (π.χ. βιογραφικό ή βιογραφικό και συστάσεις)
  - Έλεγχο ποινικού μητρώου
- Τα τρίτα μέρη που παρέχουν αναδόχους /συμβούλους απευθείας της εταιρίας που χρησιμοποιούνται από την εταιρεία θα πρέπει να εκτελούν

τουλάχιστον το ίδιο επίπεδο ελέγχου του ιστορικού, όπως αυτό που αναφέρονται παραπάνω.

- Κατάλληλη ευαισθητοποίηση, κατάρτιση και εκπαίδευση για την ασφάλεια των πληροφοριών πρέπει να παρέχεται σε όλους τους εργαζόμενους των τρίτων μερών, οι οποίοι έχουν πρόσβαση σε πόρους και πληροφορίες της εταιρείας. Στα πλαίσια της κατάρτισης του προσωπικού τρίτων μερών, θα πρέπει να διασαφηνίζονται οι αρμοδιότητες που έχουν σχετικά με πολιτικές ασφάλειας των πληροφοριών, τα πρότυπα, τις διαδικασίες και τις κατευθυντήριες γραμμές και όλες τις σχετικές υποχρεώσεις που καθορίζονται στη σύμβαση.

- **Έλεγχοι πρόσβασης.**
  - Για την αποτροπή μη εξουσιοδοτημένης πρόσβασης στους πληροφοριακούς και άλλους πόρους της εταιρείας από τρίτο πάροχο ή υπεργολάβους, απαιτούνται κατάλληλοι έλεγχοι ασφαλείας.
  - Οι απαιτήσεις ασφάλειας και οι έλεγχοι που απαιτούνται, εξαρτώνται από την κρισιμότητα και τις απαιτήσεις κάθε πόρους και κάθε πληροφορίας, σύμφωνα με ότι ορίζεται στην πολιτική ασφάλειας πληροφοριών της εταιρίας. Τα μέτρα προστασίας της εμπιστευτικότητας των πληροφοριακών και άλλων πόρων της εταιρείας μπορεί να περιλαμβάνουν:
    - Ταυτοποίηση και επαλήθευση ταυτότητας χρήστη (authentication),
    - εφαρμογή τεχνικών μέσων ελέγχου πρόσβασης και συναγερμών /προειδοποιήσεων(monitoring/alerting) σε περιπτώσεις παραβίασης πρόσβασης.
    - Επιλογή ισχυρών κωδικών πρόσβασης
    - Καθορισμό και διαμόρφωση κατάλληλων δικαιωμάτων λογικής ή/και φυσικής πρόσβασης
    - Επανεξέταση και αναθεώρηση ελέγχων πρόσβασης
  - Αν τμήματα της υποδομής της εταιρίας πρόκειται να φιλοξενηθούν σε τρίτο χώρο, ο χειριστής του κέντρου δεδομένων θα πρέπει να εξασφαλίζει ότι τα περιουσιακά στοιχεία της εταιρίας είναι τόσο φυσικά. όσο και λογικά απομονωμένα από τρίτα συστήματα.

➢ Η εταιρεία εξασφαλίζει ότι όλα τα περιουσιακά στοιχεία που παραδόθηκαν σε τρίτα μέρη στα πλαίσια υλοποίησης συμβάσεων (όπως και τυχόν αντίγραφα τους), ανακτώνται ή καταστρέφονται σε κατάλληλο σημείο κατά τη διάρκεια ή πριν από τη λήξη της σύμβασης, σύμφωνα με την Οδηγία Καταστροφής Δεδομένων.

- **Έλεγχοι ασφάλειας (Right to Audit).**

➢ Η εταιρία διατηρεί το δικαίωμα να πραγματοποιεί περιοδικούς ελέγχους σε φυσικούς χώρους του παρόχου για να διαπιστωθεί ο βαθμός συμμόρφωσης με τις πολιτικές ασφάλειας του και των απαιτήσεων που καθορίζονται στη σύμβαση.

➢ Ο έλεγχοι που θα πραγματοποιεί η εταιρία θα πρέπει να λαμβάνουν υπόψη τα επίπεδα υπηρεσιών που έχουν συμφωνηθεί στη σύμβαση, καθορίζοντας κατά πόσο έχουν τηρηθεί με συνέπεια και επανεξέταση των ελέγχων που απαιτούνται για τη διόρθωση τυχόν αποκλίσεων.

➢ Η συχνότητα των ελέγχων καθορίζεται από τον Υ.Δ.Α.Π. σύμφωνα με τις απαιτήσεις κάθε έργου και τις διαδικασίες διαχείρισης ποιότητας και ασφάλειας της εταιρίας.

- **Χρησιμοποιούμενα Έντυπα και αρχειοθέτηση**

Α/Α	ΑΡΧΕΙΟ	ΕΠΙΣΥΝΑΠΤΟΜΕΝΑ		ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ ΑΡΧΕΙΟΥ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ
		ΕΝΤΥΠΟ	ΚΩΔΙΚΟΣ		

2.5 Πολιτική κινητών συσκευών και αποθηκευτικών μέσων

Σκοπός της παρούσας πολιτικής είναι να καθορίσει τους κανόνες που θα πρέπει να τηρούνται για τον έλεγχο των κινητών συσκευών και των αφαιρούμενων αποθηκευτικών μέσων που περιέχουν πληροφορίες της εταιρίας και βρίσκονται είτε εντός, είτε εκτός των υποδομών της. Η πολιτική αυτή εφαρμόζεται σε όλη την εταιρεία και αφορά όλα τα στελέχη και το προσωπικό της εταιρείας.

2.5.1 Υπευθυνότητες

- Οι χρήστες της εατιρίας, όσον αφορά την τήρηση των όσων ορίζονται στη παρούσα πολιτική, όταν χρησιμοποιούν φορητές ή κινητές συσκευές και όταν

αποθηκεύουν δεδομένα και πληροφορίες της εταιρείας σε αφαιρούμενα αποθηκευτικά μέσα.

- Ο Υπεύθυνος Δ.Α.Π. είναι υπεύθυνος για τη συντήρηση και ενημέρωση της παρούσας πολιτικής και για τον περιοδικό επαν- υπολογισμό της επικινδυνότητας που σχετίζεται με τις κινητές συσκευές και τα αφαιρούμενα αποθηκευτικά μέσα, όπως και για τον έλεγχο της ορθής εφαρμογής των κατάλληλων μέτρων προστασίας.

2.5.2 Περιγραφή

Ορισμοί:

Κινητές Συσκευές: Ως κινητές συσκευές καθορίζονται φορητοί υπολογιστές (laptops), PDAs, κινητά τηλέφωνα, tablets και ότι άλλη φορητή συσκευή έχει επεξεργαστική ισχύ και μπορεί κάποιος χρήστης να αποθηκεύσει και να επεξεργαστεί δεδομένα

Αφαιρούμενα Αποθηκευτικά μέσα: Οπτικοί Δίσκοι (CDs, DVDs), φορητοί σκληροί δίσκοι, συσκευές USB ή όποιο άλλο μέσο μπορεί να χρησιμοποιηθεί για την αποθήκευση και μεταφορά δεδομένων.

- **Απαιτήσεις Πολιτικής**
  - Οι κινητές συσκευές και τα αφαιρούμενα αποθηκευτικά μέσα που περιέχουν ή έχουν πρόσβαση σε διαβαθμισμένες πληροφορίες της εταιρίας είναι απαραίτητο να εγκρίνονται πριν αποκτήσουν πρόσβαση στα πληροφοριακά συστήματα της εταιρείας.
  - Ο Υ.Δ.Α.Π. τηρεί και συντηρεί το Έγγραφο Επιτρεπόμενων Κινητών Συσκευών, όπου καταγράφονται τα είδη και τα λειτουργικά συστήματα κινητών συσκευών τα οποία μπορούν να χρησιμοποιηθούν από τους χρήστες της εταιρείας.
  - Η αποθήκευση ευαίσθητων πληροφοριών σε αφαιρούμενα αποθηκευτικά μέσα δεν επιτρέπεται, εκτός αν δοθεί γραπτή εξαίρεση από τον Υ.Δ.Α.Π., για την παροχή της οποίας απαιτείται να ακολουθηθεί η Διαδικασία Διαχείρισης Πρόσβασης.

➢ Οι κινητές συσκευές ή τα αφαιρούμενα αποθηκευτικά μέσα, όταν περιέχουν ευαίσθητες πληροφορίες θα πρέπει να χρησιμοποιούν κρυπτογράφηση, τουλάχιστον για τα δεδομένα αυτά.

- **Παροχή πρόσβασης σε κινητές συσκευές**

  ➢ Οι κινητές συσκευές και τα αφαιρούμενα αποθηκευτικά μέσα τα οποία χρησιμοποιούν οι χρήστες καταγράφονται σύμφωνα με τα όσα ορίζονται στη Διαδικασία Παροχής Πρόσβασης και τηρείται σχετικό αρχείο για κάθε χρήστη

  ➢ Πριν την παροχή πρόσβασης σε κάποιο νέο είδος συσκευής θα πρέπει να πραγματοποιείται αποτίμηση επικινδυνότητας που θα αποσκοπεί στην αναγνώριση κινδύνων και ευπαθειών που σχετίζονται με κάθε είδος συσκευής.

- **Απώλεια ή Κλοπή**

  ➢ Η απώλεια ή κλοπή κινητών συσκευών οι οποίες περιέχουν δεδομένα της εταιρείας ή έχουν πρόσβαση στα δίκτυα και τις υποδομές της εταιρίας θα πρέπει να δηλώνεται στον Υ.Δ.Α.Π. σύμφωνα με τα όσα ορίζονται στη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας.

  ➢ Σε περίπτωση απώλειας ή κλοπής συσκευών οι οποίες περιέχουν δεδομένα της εταιρίας, ο Υ.Δ.Α.Π. θα φροντίζει για την κατάργηση των δικαιωμάτων του χρήστη και την επικοινωνία με την Διοίκηση προκειμένου να εκκινήσει τη διαδικασία εκ νέου παροχής των προσβάσεων που έχει ο χρήστης.

- **Χρησιμοποιούμενα Έντυπα και αρχειοθέτηση**

Α/Α	ΑΡΧΕΙΟ	ΕΠΙΣΥΝΑΠΤΟΜΕΝΑ		ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ ΑΡΧΕΙΟΥ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ
		ΕΝΤΥΠΟ	ΚΩΔΙΚΟΣ		

2.6 Πολιτική απομακρυσμένης πρόσβασης

Ο σκοπός αυτής της πολιτικής είναι να καθορίσει κανόνες και απαιτήσεις που πρέπει να πληρούνται κατά τη σύνδεση στο δίκτυο της εταιρίας από σημεία εκτός αυτού. Οι κανόνες οι οποίοι αποτυπώνονται στη παρούσα πολιτική έχουν σχεδιαστεί για να ελαχιστοποιούν το ενδεχόμενο έκθεσης της εταιρείας σε ζημιές οι οποίες μπορούν να προκύψουν από τη μη εξουσιοδοτημένη χρήση των πόρων

του δικτύου της. Η πολιτική αυτή εφαρμόζεται σε όλη την εταιρεία και αφορά όλα τα στελέχη και το προσωπικό της εταιρείας.

2.6.1 Υπευθυνότητες

- Η Διοίκηση, όσον αφορά τον καθορισμό της Διαδικασίας και την αποτίμηση της αποτελεσματικότητας της καθώς και όλο το προσωπικό της εταιρείας κατά τη διεκπεραίωση των καθημερινών του καθηκόντων.
- Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών – στη συνέχεια θα αναγράφεται ως Υ.Δ.Α.Π.- και οι Διαχειριστές Δικτύου και Συστημάτων, είναι υπεύθυνοι για την ορθή τήρηση των όσων ορίζονται στη παρούσα πολιτική και για την αξιολόγηση αιτημάτων απομακρυσμένης πρόσβασης σε περίπτωση άδειας του προσωπικού, σύμφωνα με την Πολιτική Διαχείρισης Πρόσβασης σε περίπτωση άδειας του προσωπικού της εταιρίας.

2.6.2 Περιγραφή

Υπάρχουν δύο περιπτώσεις απομακρυσμένης εξωτερικής σύνδεσης στο δίκτυο της Εταιρίας:

Εργαζόμενος εκτός έδρας (σε άδεια, σε πελάτη κοκ.). Γίνεται μόνο με χρήση εταιρικού laptop. Σε περίπτωση που παραστεί η έκτακτη ανάγκη για άμεση πρόσβαση στο δίκτυο της Εταιρίας γίνεται ασφαλής σύνδεση μέσω secure VPN. Η χρήση γίνεται μέσω τηλεφωνικής γραμμής ή εταιρικού κινητού τηλεφώνου (με χρήση δικτύου κινητής τηλεφωνίας).

Πελάτες για λήψη ενημερώσεων εφαρμογών (υπό συνθήκες). Η σύνδεση γίνεται μόνο από συγκεκριμένο υπολογιστή μέσω secure VPN. Η χρήση γίνεται μέσω τηλεφωνικής γραμμής.

- **Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks)**
  - Κατά την απομακρυσμένη πρόσβαση τους, οι χρήστες της εταιρίας συνδέονται σε διαφορετικά εικονικά ιδιωτικά δίκτυα (VPN) με την εταιρία και αποκτούν διαφορετικό επίπεδο πρόσβασης, ανάλογα με το ρόλο που έχουν. Συγκεκριμένα, οι κατηγορίες χρηστών για την απομακρυσμένη πρόσβαση είναι οι παρακάτω:

- **Διοίκηση**. Συνδέονται σε σημείο του δικτύου που τους επιτρέπει την πρόσβαση σε εφαρμογές που σχετίζονται τόσο με διαχειριστικά θέματα, όσο και με οικονομικά θέματα.
- **Προσωπικό.** Συνδέονται στο δίκτυο της εταιρίας αποκτώντας πλήρη πρόσβαση στα συστήματα της εταιρείας της δικαιοδοσίας τους.

➢ Η πρόσβαση μέσω VPN στο δίκτυο της εταιρίας παρέχεται ως υπηρεσία στους χρήστες του δικτύου, πράγμα που σημαίνει ότι οι χρήστες είναι υπεύθυνοι για την επιλογή του παρόχου υπηρεσιών Διαδικτύου (ISP), την εγκατάσταση του απαιτούμενου λογισμικού σύνδεσης και της πληρωμής για την παροχή όλων των υπηρεσιών που απαιτούνται για την παροχή πρόσβασης στην υπηρεσία VPN.

➢ Καθ' όλη τη διάρκεια της απομακρυσμένης σύνδεσης ισχύουν οι απαιτήσεις και οι κατευθύνσεις που περιέχονται στην πολιτική ορθής χρήσης.

➢ Η πρόσβαση στην υπηρεσία VPN ελέγχεται με την αξιοποίηση μηχανισμών επαλήθευσης ταυτότητας των χρηστών (authentication), οι οποίο έχουν ίδιο επίπεδο ασφάλειας με τους αντίστοιχους μηχανισμούς που εφαρμόζονται για τον έλεγχο πρόσβασης στα πληροφοριακά συστήματα της εταιρείας.

➢ Κατά τη χρήση των υπηρεσιών VPN της εταιρίας δεν επιτρέπεται η σύνδεση σε τρίτα δίκτυα (dual split).

➢ Σε περίπτωση που η συσκευή που έχει πρόσβαση στην υπηρεσία VPN παραμένει ανενεργή για παραπάνω από 30 λεπτά, θα αποσυνδέεται αυτόματα από την υπηρεσία και θα απαιτείται η εκ νέου επαλήθευση της ταυτότητας του χρήστη για την επανασύνδεση.

➢ Ο εξοπλισμός που χρησιμοποιείται για την παροχή της υπηρεσίας VPN συντηρείται από εξωτερικό συνεργάτη ο οποίος έχει αξιολογηθεί.

- **Χρησιμοποιούμενα Έντυπα και αρχειοθέτηση**

Α/Α	ΑΡΧΕΙΟ	ΕΠΙΣΥΝΑΠΤΟΜΕΝΑ		ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ ΑΡΧΕΙΟΥ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ
		ΕΝΤΥΠΟ	ΚΩΔΙΚΟΣ		

2.7 Πολιτική Οργάνωσης Ασφάλειας Πληροφοριών

Σκοπός του παρόντος εγγράφου είναι να ορίσει το διοικητικό πλαίσιο το οποίο ανέπτυξε η εταιρία σχετικά με:

- Τους ρόλους και τις αρμοδιότητες που αφορούν την ασφάλεια πληροφοριών
- Τη διαχείριση των πόρων της εταιρείας
- Τις απαιτήσεις συμμόρφωσης
- Τα τρίτα μέρη

Το παρόν έγγραφο έχει εφαρμογή για το προσωπικό, τους εξωτερικούς συνεργάτες και τα τρίτα μέρη που έχουν πρόσβαση και χρησιμοποιούν πόρους της εταιρείας είτε σε μόνιμη, είτε σε προσωρινή βάση.

2.7.1 Υπευθυνότητες

Το παρόν έγγραφο, συντηρείται και ενημερώνεται από τον Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών, με την έγκριση της Διοίκησης, σύμφωνα με τη σχετική διαδικασία διαχείρισης εγγράφων.

2.7.2 Περιγραφή

- **ΟΡΓΑΝΩΣΗ ΤΟΥ Σ.Δ.Α.Π. - ΡΟΛΟΙ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ**

Κάθε εργαζόμενος στην εταιρία ανήκει σε κάποια ομάδα χρηστών του Σ.Δ.Α.Π και έχει μία σειρά συγκεκριμένων καθηκόντων και αρμοδιοτήτων που αφορούν τη Διαχείριση της Ασφάλειας Πληροφοριών. Στη συνέχεια της παραγράφου παρατίθενται οι ρόλοι χρηστών του Σ.Δ.Α.Π. της εταιρίας και οι αρμοδιότητες κάθε ρόλου.

- **Διοίκηση**

Η Διοίκηση είναι υπεύθυνη για:

➢ Την εξασφάλιση ότι οι στόχοι που σχετίζονται με την διαχείριση της ασφάλειας πληροφοριών είναι καλά ορισμένοι και ότι έχουν δημιουργηθεί και ακολουθούνται διαδικασίες που αποσκοπούν στην επίτευξη τους

- Τη διαμόρφωση, την επισκόπηση και την έγκριση των πολιτικών ασφάλειας πληροφοριών
- Την παρακολούθηση της αποτελεσματικότητας της εφαρμογής των πολιτικών ασφάλειας πληροφοριών
- Την παροχή σαφών κατευθύνσεων και την υποστήριξη των ενεργειών και λειτουργιών που σχετίζονται με την ασφάλεια πληροφοριών
- Τη διάθεση των πόρων που απαιτούνται για τη διατήρηση του επιθυμητού επιπέδου ασφάλειας πληροφοριών
- Την έναρξη και υποστήριξη ενεργειών που αποσκοπούν στην ενημέρωση του προσωπικού και των εξωτερικών συνεργατών για θέματα σχετικά με τη ασφάλεια πληροφοριών.

Επίσης έχει τις παρακάτω αρμοδιότητες:

- Να επιβλέπει την ανάπτυξη και την εφαρμογή των πολιτικών ασφάλειας
- Να εγκρίνει τις σχετικές μεθοδολογίες και διαδικασίες που ακολουθούνται για τη διαχείριση της ασφάλειας των πληροφοριών
- Να υποδεικνύει τη διαχείριση των περιστατικών μη συμμόρφωσης τα οποία εντοπίζονται
- Να αξιολογεί την επάρκεια και να συντονίζει την εφαρμογή των αντιμέτρων ασφάλειας πληροφοριών
- Να εντοπίζει σημαντικές αλλαγές στο είδος των απειλών ή στο βαθμό έκθεσης των πληροφοριών και των εγκαταστάσεων επεξεργασίας σε υφιστάμενες ή νέες απειλές
- Να παρέχει ένα σημείο αναφοράς στους χρήστες, στο οποίο θα μπορούν να αναφέρουν θέματα και να εγείρουν ζητήματα που αφορά την ασφάλεια πληροφοριών.

- **Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών (Υ.Δ.Α.Π.)**

Είναι Εκπρόσωπος Διοίκησης και ο ρόλος του είναι η επίβλεψη της εφαρμογής και η συνεχής βελτίωση ολόκληρου του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Σ.Δ.Α.Π.) σύμφωνα με τις απαιτήσεις του Προτύπου ISO 27001:2013.

Ο Υ.Δ.Α.Π. Υποστηρίζει τη Διοίκηση κατά την ανάπτυξη της στρατηγικής διαχείρισης ασφάλειας πληροφοριών, σύμφωνα με τη λειτουργία και τις ανάγκες

της εταιρείας και συνεπικουρείται από το προσωπικό του ΥΔΠ. Οι ευθύνες του Υ.Δ.Α.Π. περιλαμβάνουν:

- Τη διαχείριση των λειτουργιών που σχετίζονται με την ασφάλειας πληροφοριών, σύμφωνα με τις πολιτικές ασφάλειας του Σ.Δ.Α.Π..
- Τη δημιουργία και τήρηση του επιπέδου ασφαλείας και των διαδικασιών ασφάλειας, σύμφωνα με ότι ορίζεται στις πολιτικές ασφάλειας και σε κοινώς αποδεκτά πρότυπα και οδηγίες.
- Την υλοποίηση των ενεργειών εκτίμησης επικινδυνότητας, αξιοποιώντας εσωτερικούς ή εξωτερικούς πόρους
- Την αξιολόγηση του επιπέδου συμμόρφωσης με τις πολιτικές ασφάλειας πληροφοριών και των συναφών διαδικασιών
- Την αξιολόγηση του επιπέδου συμμόρφωσης με τη σχετική νομοθεσία και τις συμβατικές ή/και κανονιστικές απαιτήσεις της εταιρείας, σε συνεργασία με τον Υπεύθυνο Διαχείρισης Ποιότητας
- Τον συντονισμό των ενεργειών που σχετίζονται με τη διαχείριση ασφάλειας πληροφοριών, σε συνεργασία με τα κατάλληλα τμήματα της εταιρείας.
- Την παροχή περιοδικών εκθέσεων σχετικά με θέματα ασφάλειας των πληροφοριών στη Ανώτατη Διοίκηση.
- Τον συντονισμό των ενεργειών διαχείρισης ασφάλειας και των προγραμμάτων ευαισθητοποίησης για θέματα ασφάλειας.
- Την επικοινωνία με τις Αρχές και τη συνεχή επαφή με ομάδες ενδιαφέροντος και εξειδικευμένους συμβούλους ασφάλειας πληροφοριών

- **Διαχειριστές Δικτύου και Συστημάτων**

Το πληροφοριακό σύστημα της εταιρίας αποτελείται από μία σειρά επιμέρους μικρότερων υπολογιστικών, αλλά και πληροφοριακών συστημάτων, κάθε ένα εκ των οποίων επιτελεί διακριτό σκοπό, εκτελεί συγκεκριμένη λειτουργία και έχει συγκεκριμένες απαιτήσεις. Κάθε ένα από τα επιμέρους πληροφοριακά συστήματα τα οποία συνθέτουν το συνολικό πληροφοριακό σύστημα της εταιρίας έχει συνδεθεί με έναν συγκεκριμένο Επιβλέπων Προγραμματιστή, ο οποίος είναι επιφορτισμένος με τις παρακάτω ευθύνες:

- Η διασφάλιση της καλής λειτουργίας κάθε επιμέρους Πληροφοριακού Συστήματος,

- Η διαφύλαξη του αποδεκτού επιπέδου εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας του εκάστοτε συστήματος, μέσω της συμμόρφωσης με τις πολιτικές και τις διαδικασίες του Σ.Δ.Α.Π.
- Η χορήγηση του κατάλληλου επιπέδου πρόσβασης σε χρήστες ανάλογα με το ρόλο και την εργασία που επιτελούν
- Η συμμόρφωση με τις πολιτικές και διαδικασίες του Σ.Δ.Α.Π. κατά τη ρύθμιση, συντήρηση και λειτουργία των υπολογιστικών συστημάτων και των επιμέρους πληροφοριακών συστημάτων για τα οποία είναι υπεύθυνοι.

- **Χρήστες**

Αφορά οποιονδήποτε εμπλέκεται στην εφαρμογή του Σ.Δ.Α.Π. και ενδιαφέρεται για την δραστηριότητα της εταιρείας ή επηρεάζεται από αυτήν. Οι χρήστες χωρίζονται σε εσωτερικούς και εξωτερικούς ως εξής:

- Οι εσωτερικοί είναι: όλο το προσωπικό της εταιρείας και η Διοίκηση
- Οι εξωτερικοί είναι: συνεργάτες του, σύμβουλοι, προγραμματιστές, εξωτερικοί ελεγκτές.

Όλοι οι χρήστες, εσωτερικοί και εξωτερικοί, είναι υπεύθυνοι για τη συμμόρφωση των ενεργειών τους με τις πολιτικές ασφάλειας της εταιρείας και για την τήρηση των διαδικασιών ασφάλειας που ορίζονται στο Σ.Δ.Α.Π.

- **Υπεύθυνος Διαχείρισης Ποιότητας (Υ.Δ.Π.):**

Ο Υπεύθυνος Διαχείρισης Ποιότητας είναι υπεύθυνος για την λειτουργία του συστήματος ποιότητας.

- **Χρησιμοποιούμενα Έντυπα και αρχειοθέτηση**

Α/Α	ΑΡΧΕΙΟ	ΕΠΙΣΥΝΑΠΤΟΜΕΝΑ		ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ ΑΡΧΕΙΟΥ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ
		ΕΝΤΥΠΟ	ΚΩΔΙΚΟΣ		

ΕΠΙΛΟΓΟΣ

Στο τρέχον κεφάλαιο επιχειρήθηκε ο σχεδιασμός και η ανάπτυξη των πολιτικών ασφάλειας πληροφοριών της εταιρίας, σύμφωνα πάντα με τις απαιτήσεις του Κανονισμού Γενικής Προστασίας Δεδομένων (GDPR) και σε συνεργασία με το διεθνές πρότυπο ISO27001. Αναφέρθηκαν οι πολιτικές και αναπτύχθηκαν ο σκοπός, το πεδίο εφαρμογής τους και βεβαίως έγινε αναλυτική περιγραφή των επιμέρους τμημάτων και χαρακτηριστικών τους.

Στη συνέχεια θα προχωρήσουμε στη σύνταξη καταλόγου και αναλυτική περιγραφή όλων των διαδικασιών προστασίας δεδομένων που ο Γενικός Κανονισμός σε συνεργασία με το διεθνές πρότυπο εφαρμόζει στην εταιρία της εργασίας μας.

ΚΕΦΑΛΑΙΟ 3

Κατάλογος διαδικασιών προστασίας δεδομένων & υλοποίηση της πολιτικής ασφαλείας

ΕΙΣΑΓΩΓΗ

Η διαδικασία προστασίας δεδομένων είναι ένας καθορισμένος τρόπος για την εκτέλεση μιας δραστηριότητας ή μίας διεργασίας όπως η πολιτική ασφαλείας.

Θα πρέπει να έχουμε υπόψη μας βεβαίως, τους όρους που χρησιμοποιούνται σε ένα σύστημα διαχείρισης ασφάλειας πληροφοριών, ώστε να επιτευχθεί η προστασία δεδομένων μας. Παρακάτω γίνεται μια συνοπτική παρουσίαση τους:

- **Περιουσιακά στοιχεία– αγαθά (assets):** Κάθε τι που έχει αξία για την εταιρεία. Χαρακτηρίζονται σε:
  - **Δεδομένα (Data assets)** - κάθε είδους δεδομένα (βάση δεδομένων, καταχωρήσεις σε server, κ.α).
  - **Υπηρεσίες (End User Services)**: Αφορούν τις υπηρεσίες που επιτρέπουν στον τελικό χρήστη πρόσβαση στα δεδομένα (π.χ. υπηρεσία πρόσβασης σε βάση δεδομένων που επιτρέπει στους χρήστες πρόσβαση στα δεδομένα).
  - **Υλικά Στοιχεία**: Περιλαμβάνει στοιχείων των υπολογιστικών συστημάτων όπως, Η/Υ, δίκτυο, μέσα αποθήκευσης, κ.α.
  - **Τοποθεσίες**: Χώροι, κτίρια και δομές που ανήκουν στην εταιρεία και περιέχουν μέρη των υπολογιστικών συστημάτων.
  - **Λογισμικό (software)**: Αφορά στην προστασία του κώδικα.
- **Εμπιστευτικότητα (Confidentiality):** Η ιδιότητα των δεδομένων να καθίστανται αναγνώσιμα μόνο από εξουσιοδοτημένα λογικά υποκείμενα, όπως φυσικές οντότητες και διεργασίες λογισμικού.
- **Διαθεσιμότητα (Availability):** Η αποτροπή της προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε κάθε εξουσιοδοτημένο λογικό υποκείμενο του συστήματος.
- **Ακεραιότητα (Integrity):** Είναι η ιδιότητα των δεδομένων να υφίστανται σε προκαθορισμένο φυσικό μέσο ή χώρο και να είναι ακριβή. Δηλαδή η μη-εξουσιοδοτημένη τροποποίηση της πληροφορίας θα πρέπει να

αποτρέπεται, ενώ κάθε αλλαγή του περιεχομένου των δεδομένων να είναι αποτέλεσμα εξουσιοδοτημένης και ελεγχόμενης ενέργειας.

- **Ασφάλεια Πληροφοριών (information security):** Η ασφάλεια των πληροφοριών αναφέρεται στην προστασία της πληροφορίας στην ολότητά της και των σχετικών με την ασφάλεια ιδιοτήτων. Ως θεμελιώδεις ιδιότητες ασφάλειας θεωρούνται η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα.
- **Ευπάθεια (volnerability):** Αδυναμία ή σχεδιαστική ατέλεια σε ένα σύστημα, στην εφαρμογή ή στην υποδομή που μπορεί να γίνει αιτία παραβίασης.
- **Απειλή (threat):** Μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα εξοπλισμού, συστημάτων, υπηρεσιών, και δεδομένων, που εμφανίζεται τυχαία ή με πρόθεση και δύναται να αλλοιώσει ή/και να καταστρέψει δεδομένα, καθώς και η μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών.
- **Κίνδυνος (risk):** Η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια και ενδεχομένως να προκληθεί απώλεια.
- **Ανάλυση επικινδυνότητας (risk analysis):** Συστηματική χρήση πληροφοριών για την αναγνώριση και αποτίμηση πηγών κινδύνου και υπολογισμού του μεγέθους του. Αποσκοπεί στη γενικότερη βελτίωση της ασφάλειας πληροφοριακών συστημάτων.
- **Αξιολόγηση επικινδυνότητας (risk assessment):** Συνολική Διεργασία για την ανάλυση επικινδυνότητας και την αξιολόγηση κινδύνων.
- **Διαθεσιμότητα (availability):** Εξασφάλιση της διαθεσιμότητας Η/Υ, Συστημάτων, δικτύων, και δεδομένων σε εξουσιοδοτημένους χρήστες όποτε απαιτείται η χρήση τους.
- **Μέτρα ασφαλείας (security measures):** Η πολιτική ασφαλείας συμπληρώνεται από τα Μέτρα Ασφαλείας ή Αντίμετρα (countermeasures). Αφορούν όλες τις διαδικασίες, τις τεχνικές, τις ενέργειες και τις συσκευές και αποσκοπούν στο να περιορίζουν τις ευπάθειες και τις απειλές του πληροφοριακού συστήματος.

  Τα Μέτρα Ασφαλείας χωρίζονται σε 4 μεγάλες κατηγορίες:

  α) **Πρόληψη:** αποσκοπούν στο να μειώσουν τον κίνδυνο

β) **Διασφάλιση:** εργαλεία, έλεγχοι και στρατηγικές που διασφαλίζουν την συνεχή αποτελεσματικότητα των Μέτρων Ασφαλείας

γ) **Ανίχνευση:** προγράμματα και τεχνικές για την έγκαιρη ανίχνευση, αναχαίτιση και αντιμετώπιση περιστατικών

δ) **Επαναφορά:** διαδικασίες που στοχεύουν στην γρήγορη επαναφορά σε ένα ασφαλές περιβάλλον έπειτα από ρήξη ασφαλείας και στον εντιπισμό της αιτίας που την προκάλεσε.

3.1 Διαχείριση εγγράφων και αρχείων

Η διαδικασία αυτή περιγράφει τον τρόπο με τον οποίο γίνεται ο έλεγχος των εγγράφων και αρχείων, έτσι ώστε να διασφαλίζεται ότι η διαχείρισή τους γίνεται με συστηματικό και ελεγχόμενο τρόπο.

Ως Έγγραφα του Συστήματος ορίζονται όλα εκείνα τα οποία συναποτελούν τα τρία βασικά επίπεδα τεκμηρίωσης και είναι τα ακόλουθα:

- Εγχειρίδιο Διαχείρισης Ποιότητας
- Διαδικασίες Συστήματος
- Λειτουργικά Έντυπα, Οδηγίες Εργασίας

Ως Ελεγχόμενα Αντίγραφα ορίζονται όλα εκείνα για τα οποία υπάρχει ρητή απαίτηση ενημέρωσης των κατόχων τους σε περίπτωση τροποποίησης ή αλλαγής τους.

Ως μη Ελεγχόμενα Αντίγραφα ορίζονται όλα εκείνα τα οποία παρέχονται σε τρίτους για πληροφοριακούς ή άλλους λόγους και για τα οποία δεν υφίσταται υποχρέωση της εταιρίας για ενημέρωση των παραληπτών τους σε κάθε πιθανή αλλαγή ή τροποποίησή τους.

Ως μη Ισχύοντα Αντίγραφα ορίζονται όλα εκείνα τα οποία δεν είναι σε ισχύ είτε διότι έχουν καταργηθεί είτε διότι έχουν τροποποιηθεί.

Κωδικοποίηση Εγγράφων

Το Εγχειρίδιο, οι Διαδικασίες, οι Οδηγίες και τα Έντυπα, αναγνωρίζονται από:

- τον τίτλο
- τον κωδικό

- την έκδοση
- την ημ/νία έκδοσης

Ο κωδικός αποτελείται από ένα πρόθεμα και έναν αριθμό:

- Δ = Διαδικασία
- ΟΕ = Οδηγία εργασίας
- Ε = Έντυπο

Ο αριθμός είναι ο αύξοντας αριθμός του εγγράφου, πχ.:

Δ-05 : είναι η 5η διαδικασία του Συστήματος Ποιότητας

Ε-05-01: το πρώτο από τα έντυπα που αντιστοιχεί στη Διαδικασία Δ-05

Συγγραφή, Έγκριση και Έκδοση Εγγράφων, Διανομή.

Οποιοδήποτε άτομο μπορεί να προτείνει νέα έγγραφα ή αλλαγές στα ήδη υπάρχοντα στον Υπεύθυνο Διαχείρισης Ποιότητας (ΥΔΠ) και στον Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών (ΥΔΑΠ) .

Υπεύθυνος για την συγγραφή και την διανομή των εγγράφων είναι ο Υπεύθυνος Διαχείρισης Ποιότητας και ο Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών (ΥΔΑΠ). Υπεύθυνος για την έγκριση και έκδοση των εγγράφων είναι ο Γενικός Διευθυντής. Το σύνολο των εντύπων διακινούνται σε ηλεκτρονική μορφή : σε .doc ή .xls αρχεία όσα είναι προς συμπλήρωση και σε .pdf αρχεία όσα είναι προς αποθήκευση.

Μικρές αλλαγές στα ισχύοντα έγγραφα του Συστήματος επιτρέπονται, με την προϋπόθεση ότι αυτές ελέγχονται από τον ΥΔΠ και τον ΥΔΑΠ. Αυτοί φροντίζουν οι αλλαγές να αναγραφούν σε όλα τα κυκλοφορούντα αντίγραφα, φέροντας δίπλα την ημερομηνία και την υπογραφή τους.

Οι ανάγκες τροποποίησης εγγράφων του τηρουμένου Συστήματος, μπορεί να προκύψουν από:

- Αλλαγές στον τρόπο λειτουργίας της εταιρείας.
- Μη ικανοποίηση κάλυψης των αναγκών του εκάστοτε τμήματος.
- Μη-Συμμορφώσεις και επακόλουθες Διορθωτικές Ενέργειες.

Η διανομή των εντύπων γίνεται ηλεκτρονικά μέσω e-email στους υπεύθυνους τεκμηρίωσης της εκάστοτε διαδικασίας και παρακολουθείται από τον ΥΔΠ και τον ΥΔΑΠ.

Εξωτερικά έγγραφα

Τα εξωτερικά έγγραφα από Πελάτες τηρούνται σε ηλεκτρονική μορφή στους λογαριασμούς e-mail της εταιρείας info@etairia.gr, support@etairia.gr, fax@etairia.gr, κ.λ.π.., ώστε να είναι άμεσα προσβάσιμα σε όλους τους εμπλεκόμενους εργαζόμενους της εταιρείας. Νομοθεσίες, Κανονισμοί, Οδηγίες που εκδίδονται από Φορείς Εκτελεστικής και Νομοθετικής Εξουσίας, όπως επίσης και από την ΕΕ και με τα οποία είναι υποχρεωμένη να συμμορφωθεί η εταιρεία, καταγράφονται και παρακολουθούνται από τον ΥΔΠ και τον ΥΔΑΠ και αποστέλλονται με e-mail σε όλους τους εργαζόμενους της εταιρείας.

Τήρηση αρχείων

Το σύνολο των αρχείων είναι ηλεκτρονικής μορφής. Το σύνολο των αρχείων είναι καθορισμένα. Τα ηλεκτρονικά αρχεία προστατεύονται με την τήρηση back up κάθε εβδομάδα. Την γενική εποπτεία των αρχείων που τηρούνται έχει ο ΥΔΠ και ο ΥΔΑΠ.

Η τήρηση των Αρχείων στοχεύει στη συλλογή όλων των κρίσιμων πληροφοριών για την λειτουργία του Συστήματος Διαχείρισης Ποιότητας και του Συστήματος Ασφάλειας Πληροφοριών, προκειμένου αυτά να αναλυθούν και να αξιολογηθούν για την περαιτέρω αξιολόγησή τους για την επίτευξη της συνεχούς βελτίωσης (continual improvement) της αποτελεσματικότητάς του.

Επίσης, τα Αρχεία έχουν το ρόλο της απόδειξης της εφαρμογής και τήρησης των Συστημάτων σε επιθεωρήσεις δεύτερου μέρους (2nd party audits), από πελάτες (υπάρχοντες ή δυνητικούς) ή επιθεωρήσεις τρίτου μέρους (3rd party audits) από φορείς πιστοποίησης για λήψη πιστοποιητικού σχετικά με τη συμμόρφωση στις απαιτήσεις του Προτύπου ISO 27001.

Τέλος, με την τήρηση των Αρχείων διασφαλίζεται η δυνατότητα ιχνηλασιμότητας των προϊόντων που παρέχονται στους πελάτες αλλά και η σωστή λειτουργία της εταιρείας σε ότι αφορά την Ασφάλεια Πληροφοριών.

3.2 Ανασκόπηση της διοίκησης

Η ανασκόπηση του Συστήματος Διαχείρισης Ποιότητας και Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών που εφαρμόζει η Εταιρεία, εκτελείται για να διασφαλισθεί ότι αυτό παραμένει αποτελεσματικό, δυναμικό και αντικατοπτρίζει κάθε αλλαγή στη φιλοσοφία ή στην πολιτική ποιότητας. Περιγράφει τον τρόπο με τον οποίο γίνεται η ανασκόπηση του Συστήματος.

Στην ανασκόπηση από τη Διοίκηση συμμετέχουν τα μέλη της Ομάδας Ποιότητας.

Ο τρόπος με τον οποίο γίνεται η ανασκόπηση από την Διοίκηση είναι απόλυτα προσδιορισμένος και αυτό διασφαλίζεται από την ύπαρξη εγγράφου που συμπληρώνεται σε κάθε ανασκόπηση και καλύπτει όλα τα στοιχεία που αφορούν και συνθέτουν το σύστημα. Ανασκόπηση από την Διοίκηση γίνεται τουλάχιστον μία φορά κατά την διάρκεια του έτους.

Τα στοιχεία που καλύπτονται και καταγράφονται με ακρίβεια είναι :

- Τα εισερχόμενα στη Διεργασία ανασκόπησης, που είναι τα εξής:
  - Επακόλουθες ενέργειες από προηγούμενες ανασκοπήσεις από την διοίκηση.
  - Εξωτερικές ή εσωτερικές επιθεωρήσεις.
  - Ανατροφοδότηση από τον πελάτη.
  - Επίδοση διεργασιών και συμμόρφωση προϊόντος – υπηρεσίας.
  - Κατάσταση προληπτικών και διορθωτικών ενεργειών.
  - Αλλαγές που θα μπορούσαν να επηρεάσουν το σύστημα διαχείρισης της ποιότητας.
  - Συστάσεις για βελτίωση.

Τα εισερχόμενα αναλύονται από την Ομάδα Ποιότητας.

- Τα εξερχόμενα από την ανασκόπηση, που περιλαμβάνουν αποφάσεις και ενέργειες σχετικές με τα εξής:
  - Βελτίωση της αποτελεσματικότητας του συστήματος διαχείρισης ποιότητας και των διεργασιών του.
  - Βελτίωση του προϊόντος, η οποία σχετίζεται με τις απαιτήσεις των πελατών.

- Ανάγκες σε πόρους.

Οι ενέργειες προς εφαρμογή που αποφασίζονται κατά την ανασκόπηση του συστήματος έχουν συγκεκριμένο χρονοδιάγραμμα, υπεύθυνο υλοποίησης και κοινοποιούνται στο εμπλεκόμενο προσωπικό.

3.3 Εσωτερική & Εξωτερική επικοινωνία

Η διαδικασία καθορίζει τους τρόπους και τις μεθόδους με τις οποίες διασφαλίζεται η επικοινωνία ανάμεσα στο προσωπικό της εταιρείας, η επικοινωνία της Ομάδας Ποιότητας, καθώς και η εξωτερική επικοινωνία με πελάτες, αρμόδιες αρχές και άλλους φορείς. Τέλος αναφέρεται στην ικανότητα του οργανισμού να προσδιορίζει τις απαραίτητες γνώσεις για την λειτουργία των διεργασιών του και την επίτευξη συμμόρφωσης των προϊόντων και υπηρεσιών.

- **Εσωτερική επικοινωνία**

Ο Υπεύθυνος Διαχείρισης Ποιότητας παρακολουθεί και συντονίζει όλα τα θέματα.
Δεν υπάρχουν συγκεκριμένες και προκαθορισμένες χρονικές στιγμές επαφών διότι εξαρτώνται από την κάθε εποχή, τις αλλαγές και τις έκτακτες καταστάσεις.
Μορφές επικοινωνίας είναι τα σημειώματα, φαξ, ανακοινώσεις, e-mail, τηλεφωνήματα.
Η σύνθεση της Ομάδας Ποιότητας αποτελείται από στελέχη της εταιρίας και από εξειδικευμένους εξωτερικούς συνεργάτες.
Οι συναντήσεις της Ομάδας Ποιότητας υλοποιούνται σε τυχαία χρονικά διαστήματα, σύμφωνα με τις ανάγκες του ΣΔΠ, και συνοδεύονται από πρακτικά. Τα συμπεράσματα αναλύονται κατά την ανασκόπηση της Διοίκησης.

- **Εξωτερική επικοινωνία**

Η εξωτερική επικοινωνία αφορά την αποτελεσματική επικοινωνία με τους εξής:

- προμηθευτές και υπεργολάβους,
- πελάτες, ειδικότερα για πληροφορίες σε σχέση με τα προϊόντα (προδιαγραφές & σήμανση προϊόντων), συμβόλαια ή χειρισμό παραγγελιών συμπεριλαμβανομένων τροποποιήσεων, την ικανοποίηση του πελάτη συμπεριλαμβανομένων των παραπόνων,

- αρμόδιες αρχές (Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης κ.α.),
- άλλους οργανισμούς που επηρεάζουν ή μπορεί να επηρεαστούν από την αποτελεσματικότητα και την επικαιροποίηση των συστημάτων (φορείς πιστοποίησης).

Η εξωτερική επικοινωνία παρέχει πληροφόρηση (από και προς την εταιρία) σε θέματα ποιότητας των προϊόντων της εταιρίας. Ιδιαίτερη έμφαση δίνεται στους δυνητικούς κινδύνους που χρειάζεται να βρίσκονται υπό έλεγχο από άλλους οργανισμούς (μεταφορείς, πελάτες) σε όλο το δίκτυο διανομής.

Ο Υπεύθυνος Διαχείρισης Ποιότητας είναι υπεύθυνος για την εξωτερική επικοινωνία με όλα τα μέρη.

Μέρος της εξωτερικής επικοινωνίας είναι και η παρακολούθηση της νομοθεσίας (Κοινοτική, Εθνική), η οποία αποστέλλεται στην εταιρεία κυρίως από τα νοσοκομεία με τα οποία συνεργάζεται προκειμένου να ενημερωθούν αντίστοιχα οι κατάλληλες εφαρμογές.. Η λίστα με τις νομοθεσίες που αφορούν την εταιρία είναι ελεγχόμενο έγγραφο της διαδικασίας ελέγχου εγγράφων και αρχείων.

Η πληροφόρηση που συλλέγεται από την εξωτερική επικοινωνία συγκεντρώνεται σε μορφή αρχείου από τον Υπεύθυνο Διαχείρισης Ποιότητας.

Τα σημαντικά ζητήματα που αφορούν στη σχέση Πελατών – Εταιρίας καταγράφονται καθημερινά με τη χρήση των εργαλείων αμφίδρομης επικοινωνίας με τους πελάτες (Help Desk).

Η ικανοποίηση καθώς των πελατών προκύπτει στατιστικά και σε ετήσια βάση από τα δεδομένα των παραπάνω εργαλείων και με ευθύνη του ΥΔΠ, τηρείται σε έντυπο. Ακολουθεί η ανάλυση των αποτελεσμάτων από τον ΥΔΠ και η περαιτέρω ανάλυση κατά την ανασκόπηση του συστήματος.

Επιπλέον, τα παράπονα των πελατών παρακολουθούνται και μέσω εντύπου, το οποίο αποστέλλεται ετησίως στους πελάτες.

Από την καθημερινή χρήση των παραπάνω εργαλείων προκύπτουν και τα παράπονα των πελατών. Η ικανοποίηση των παραπόνων αυτών επαφίεται στους προγραμματιστές και τους επιβλέποντες προγραμματιστές, η οποία τηρείται αυτοματοποιημένα με τη χρήση των ιδίων εργαλείων.

Επιπλέον, τα παράπονα των πελατών παρακολουθούνται και μέσω του δεύτερου εντύπου, όταν το κρίνει ο ΥΔΠ.

Όσα παράπονα δεν δύναται να ικανοποιηθούν παρακολουθούνται μέσω εντύπου, Αντιμετώπιση μη – συμμορφώσεων, με ευθύνη του ΥΔΠ.

Τα στοιχεία της εξωτερικής επικοινωνίας εξετάζονται κατά την ανασκόπηση της Διοίκησης.

- **Επιχειρησιακή γνώση**

Ο τρόπος απόκτησης επιχειρησιακής γνώσης της εταιρίας βασίζεται τόσο σε εσωτερικές όσο και σε εξωτερικές πηγές.

Α) Εσωτερικές πηγές:

- Εμπειρία, εκπαίδευση και επιμόρφωση των στελεχών και των εργαζομένων της εταιρίας.
- Αναφορές εσωτερικών επιθεωρήσεων και αναλύσεις αναφορών μη συμμορφώσεων – διορθωτικών / προληπτικών ενεργειών και ανασκοπήσεων από την διοίκηση.
- Πνευματικά δικαιώματα εφαρμογών.

Β) Εξωτερικές πηγές:

- Νομοθεσία και κανονιστικές υποχρεώσεις που διέπουν τα προϊόντα και τις υπηρεσίες της εταιρίας.
- Πρότυπα και διαδίκτυο.
- Εξωτερικές επιθεωρήσεις και έλεγχοι.

Όλα τα παραπάνω παρακολουθούνται και ενημερώνονται από την ομάδα διαχείρισης ποιότητας και είναι διαθέσιμα στο αρχείο του οργανισμού.

3.4 Εκπαίδευση προσωπικού

Σκοπός της διαδικασίας είναι να περιγράψει το σύστημα που εφαρμόζει η εταιρεία για την ανίχνευση των αναγκών εκπαίδευσης του προσωπικού, την επιλογή των προγραμμάτων και των εκπαιδευτών, τον προγραμματισμό και διεξαγωγή της εκπαίδευσης, την αξιολόγηση των προγραμμάτων εκπαίδευσης, καθώς και την εκπαίδευση νέων υπαλλήλων, όσο αφορά στην εφαρμογή του Συστήματος Διαχείρισης Ποιότητας.

Το προσωπικό πρέπει να διαθέτει τα απαραίτητα προσόντα που καθορίζονται στην περιγραφή θέσεων εργασίας. Το προσωπικό αξιολογείται κατά την

πρόσληψη του. Για τον σκοπό της αξιολόγησης υποβάλλονται από τον ενδιαφερόμενο στοιχεία αξιολόγησης (βιογραφικό σημείωμα ή / και πιστοποιητικά σπουδών και προϋπηρεσίας), που αποδεικνύουν την ικανοποίηση των προσόντων της αντίστοιχης θέσης.

Κάθε νέος εργαζόμενος με την άφιξη του στην εταιρεία, εκπαιδεύεται με ευθύνη του ΥΔΠ. Το περιεχόμενο και η διάρκεια της εκπαίδευσης του καθορίζεται από το είδος της εργασίας και περιλαμβάνει τα εξής:

- Εκπαίδευση πάνω στη συγκεκριμένη εργασία την οποία καλείται να εκτελέσει
- Εκπαίδευση πάνω στις διαδικασίες του συστήματος διαχείρισης ποιότητας

Μετά το πέρας της εκπαίδευσης ο ΥΔΠ συμπληρώνει την Καρτέλα Εκπαίδευσης Εργαζομένου.

Η εταιρία φροντίζει να εκπαιδεύει το προσωπικό της σε περίπτωση αλλαγών όσον αφορά το σύστημα διαχείρισης ποιότητας και όταν εισάγονται νέοι τρόποι εκτέλεσης των εργασιών.

Ο Υπεύθυνος Διαχείρισης Ποιότητας, εισηγείται εκπαιδευτικά προγράμματα με βάση τις γνώσεις, την εμπειρία και την υπάρχουσα εκπαίδευση των εργαζομένων.

Στην Ανασκόπηση της Διοίκησης αξιολογείται η εκπαίδευση του προσωπικού και εξετάζονται συνολικά οι εκπαιδευτικές ανάγκες του προσωπικού.

Κατόπιν δημιουργείται το πρόγραμμα με τις προγραμματισμένες εκπαιδεύσεις του προσωπικού. Το πρόγραμμα μπορεί να διαμορφωθεί και να τροποποιηθεί καθ' όλη την διάρκεια του έτους.

Οι εισηγητές μπορεί να είναι στελέχη ή εξωτερικοί συνεργάτες και η εκπαίδευση μπορεί να λάβει χώρα στις εγκαταστάσεις της εταιρείας ή σε κάποιο εξωτερικό χώρο εκπαίδευσης.

Η αξιολόγηση εκπαίδευσης του προσωπικού πραγματοποιείται από τους επικεφαλείς των τμημάτων και τον ΥΔΠ κατά την ανασκόπηση.

3.5 Προμήθειες & αξιολόγηση προμηθευτών

Η διαδικασία καθορίζει τους τρόπους και τις μεθόδους με τις οποίες διασφαλίζεται η έγκαιρη και έγκυρη προμήθεια προϊόντων και υπηρεσιών, καθώς και η συνεχής αξιολόγηση των προμηθευτών.

Η εταιρεία θέτει ως βασικούς προμηθευτές της, εταιρείες που διαπραγματεύονται υλικό και εξοπλισμό για ηλεκτρονικούς υπολογιστές (software και hardware). Οι προμηθευτές της εταιρείας είναι σταθεροί. Σε περίπτωση που εντοπιστεί η ανάγκη για κάποιο νέο προϊόν ή υπηρεσία από οποιονδήποτε προγραμματιστή ή τεχνικό αυτή καταλήγει στον ΥΔΠ, ο οποίος είναι και ο υπεύθυνος διαχείρισης των προμηθειών. Επίσης κάποια ανάγκη προμήθειας μπορεί να προκύψει και από κάποιο δημόσιο διαγωνισμό, για τους οποίους ενημερώνεται ο ΥΔΠ και βάση των απαιτήσεων του διαγωνισμού αναζητά τον «κατάλληλο» προμηθευτή.
Αυτό σημαίνει ότι ο ΥΔΠ διενεργεί έρευνα αγοράς για πιθανές προσφορές τουλάχιστον από 2 προμηθευτές, εφόσον υπάρχουν. Ακολουθεί η αξιολόγηση του εν δυνάμει προμηθευτή και τέλος ο ΥΔΠ εισηγείται στη διοίκηση η οποία εγκρίνει ή όχι τη συγκεκριμένη προμήθεια.

Οι παραγγελίες για τον κυρίως εξοπλισμό γίνονται ετησίως ενώ οι παραγγελίες στα βοηθητικά αναλώσιμα γίνονται σε όλη την διάρκεια της χρονιάς σύμφωνα με την ζήτηση που υπάρχει και σύμφωνα με τις ανάγκες της εταιρείας,

Η αξιολόγηση προμηθευτή περιλαμβάνει:

- Αξιολόγηση της φερεγγυότητας του προμηθευτή
- Αξιολόγηση των τεχνικών μέσων του προμηθευτή και της ικανότητας του να πραγματοποιεί έγκαιρα τις παραδόσεις των προμηθειών ή να παρέχει έγκαιρα τις υπηρεσίες

Τα κριτήρια αρχικής αξιολόγησης είναι:

- Ιστορική αξιοπιστία συνεργασίας
- Οι υποδομές (Εγκαταστάσεις, μηχανολογικός εξοπλισμός) του προμηθευτή και η ικανότητα να παραδίδει έγκαιρα τις προμήθειες -υπηρεσίες σύμφωνα με τις απαιτήσεις και τις προδιαγραφές της εταιρίας.
- Συγκριτικά πλεονεκτήματα έναντι του ανταγωνισμού.
- Το κοστολόγιο.
- Η συμβατότητα του προϊόντος με τις ανάγκες της εταιρείας,
- Η εξυπηρέτηση κατόπιν αγοράς του προϊόντος.
- Πιστοποιητικά ποιότητας της εταιρείας ή των προϊόντων της.
- Τήρηση των νομικών υποχρεώσεων του προμηθευτή όσον αφορά το προϊόν.

Στους προμηθευτές αποστέλλεται Ερωτηματολόγιο Αξιολόγησης Προμηθευτή
Η βαθμολογία διαμορφώνεται ως εξής:

ΕΡΩΤΗΣΗ	ΝΑΙ	ΟΧΙ
1	5 Πόντοι	0 Πόντοι
2	5 Πόντοι	0 Πόντοι
3-10	1 Πόντος	0 Πόντοι

Η αξιολόγηση πραγματοποιείται ως εξής:

0-5 πόντοι	Μη αποδεκτός
5-10 πόντοι	Αποδεκτός

Η επαναξιολόγηση των παραπάνω γίνεται ετησίως με βάση το ερωτηματολόγιο επαναξιολόγησης προμηθευτή

Τα στοιχεία για την επαναξιολόγηση προκύπτουν από:

- Τα μη συμμορφούμενα προϊόντα-υπηρεσίες.
- Την ικανότητα του προμηθευτή να ικανοποιεί τις ανάγκες της εταιρίας σε παραδόσεις-παροχές.
- Το κόστος σε σχέση με το επίπεδο της υπηρεσίας ή του προϊόντος

Η βαθμολογία που πρέπει να έχει ένας προμηθευτής για να παραμείνει στον κατάλογο των εγκεκριμένων είναι min Μ.Ο.=1,5.

Ο προμηθευτές που πληρούν τα κριτήρια με βάση τα ερωτηματολόγια, εντάσσονται στον κατάλογο εγκεκριμένων προμηθευτών.

Σε περίπτωση που ο ΥΔΠ κρίνει μη εφικτή και λειτουργική τη χρησιμοποίηση του εντύπου για την αξιολόγηση των νέων προμηθευτών, χρησιμοποιεί το έντυπο της επαναξιολόγησης κατόπιν συνεννόησης με τους αρμοδίους προγραμματιστές και υπεύθυνους τμημάτων, ακολουθώντας την διαδικασία.

3.6 Έλεγχος μη συμμορφώσεων – Διορθωτικές & προληπτικές ενέργειες

Η διαδικασία περιγράφει τον τρόπο εντοπισμού των μη συμμορφώσεων, την καταγραφή τους, την έρευνα για την ανεύρεση της καλύτερης οριστικής λύσης, την εφαρμογή και αξιολόγηση των διορθωτικών και προληπτικών ενεργειών.

Οι μη συμμορφώσεις είναι δυνατό ενδεικτικά να αφορούν:

- Η μη – ικανοποίηση παραπόνων πελατών, όπως αυτά προκύπτουν από τη Διεργασία εσωτερικής και εξωτερικής επικοινωνίας
- Προβλήματα από εσωτερικές επιθεωρήσεις ή από επιθεωρήσεις από τρίτους (πελάτες, φορείς)
- Εφαρμογές συστημάτων (software) οποία δε λειτουργούν σωστά και απρόσκοπτα και επηρεάζουν άμεσα την ποιότητα των υπηρεσιών
- Συνεργασίες μεταξύ των τμημάτων της επιχείρησης και των εργαζομένων που απασχολούνται σε αυτά οι οποίες δεν καλύπτουν τις τεθείσες προδιαγραφές.

Οι μη συμμορφώσεις οδηγούν σε διορθωτικές ενέργειες, όταν διαπιστωθεί ότι κάποια φάση δεν εκτελέσθηκε σωστά ή καθυστέρησε αδικαιολόγητα ή όταν κάποια υπηρεσία-εφαρμογή δεν πληροί τις προδιαγεγραμμένες απαιτήσεις, και σε προληπτικές ενέργειες, όταν διαπιστωθεί η ύπαρξη αποτελεσματικότερου τρόπου εργασίας, αποδοτικότερη χρήση των εφαρμογών κ.λ.π. Οι ενέργειες για τον εντοπισμό και την εξάλειψη της αιτίας της μη συμμόρφωσης, την πρόληψη της επανεμφάνισης και της επαναφοράς της διεργασίας ή του συστήματος υπό έλεγχο έχουν ως εξής:

- Ανασκόπηση των μη συμμορφώσεων (συμπεριλαμβανομένων των παραπόνων των πελατών)
- Ανασκόπηση των τάσεων, στα αποτελέσματα παρακολούθησης, που μπορεί να δεικνύουν μετατόπιση προς απώλεια ελέγχου
- Προσδιορισμός των αιτιών της μη συμμόρφωσης.
- Αξιολόγηση της ανάγκης λήψης μέτρων, για να διασφαλίζεται η μη επανεμφάνιση της μη συμμόρφωσης
- Επιλογή και εφαρμογή των αναγκαίων μέτρων
- Ανασκόπηση των λαμβανόμενων διορθωτικών μέτρων για την διασφάλιση της αποτελεσματικότητάς τους

Η παρακολούθηση και η τεκμηρίωση των παραπάνω γίνεται μέσω του εντύπου Αντιμετώπιση μη συμμόρφωσης

Για όλες τις περιπτώσεις μη συμμορφούμενων υπηρεσιών υπάρχει:

- Άμεση τεχνική υποστήριξη επιτόπια ή τηλεφωνική

Η εκτίμηση και η επιλογή διαχείρισης του μη συμμορφούμενου προϊόντος-υπηρεσίας γίνεται με απόφαση που λαμβάνεται από τον Διευθύνοντα Σύμβουλο. Η παρακολούθηση και η επαλήθευση των διορθώσεων & διορθωτικών ενεργειών που έχουν ορισθεί, υλοποιείται από τον Υπεύθυνο Διαχείρισης Ποιότητας.

Όλες οι υλοποιούμενες διορθωτικές και προληπτικές ενέργειες, καθώς και οι τάσεις που ενδεχομένως δείχνουν μετατόπιση προς απώλεια ελέγχου, αποτελούν εισερχόμενα στην ανασκόπηση της Διοίκησης.

3.7 Εσωτερική επιθεώρηση

Η περιγραφή της δραστηριότητας των Εσωτερικών Επιθεωρήσεων του Συστήματος Διαχείρισης Ποιότητας. Ο προγραμματισμός, η προετοιμασία και η εκτέλεση των επιθεωρήσεων στα διάφορα τμήματα της εταιρείας για να διαπιστωθεί η συμμόρφωση προς το ΣΔΠ και η επιβολή διορθωτικών ενεργειών ώστε να εξαλειφθούν οριστικά οι μη συμμορφώσεις που ανακαλύφθηκαν κατά την επιθεώρηση.

Την ευθύνη για τον προγραμματισμό των εσωτερικών επιθεωρήσεων ποιότητας έχει ο Υπεύθυνος Διαχείρισης Ποιότητας.

Ο ΥΔΠ καταρτίζει το ετήσιο πρόγραμμα επιθεωρήσεων που ορίζει τις επιθεωρήσεις που θα γίνουν, καθώς και τον επιθεωρητή που θα τις εκτελέσει. Ο Επιθεωρητής πρέπει να έχει τις απαιτούμενες ικανότητες (π.χ. σεμινάριο εσωτερικών επιθεωρητών) και να μην εμπλέκεται στο επιθεωρούμενο τμήμα, ώστε να εξασφαλιστεί η αντικειμενικότητα της επιθεώρησης . Ο επιθεωρητής μπορεί να είναι είτε από την εταιρία είτε εξωτερικός συνεργάτης που θα πληροί τις προϋποθέσεις. Το πρόγραμμα εσωτερικών επιθεωρήσεων κοινοποιείται σε όλα τα τμήματα που θα επιθεωρηθούν και στους επιθεωρητές και κάθε αλλαγή του επίσης κοινοποιείται.

Η συχνότητα των επιθεωρήσεων καθορίζεται από τον ΥΔΠ, ανάλογα με την κρισιμότητα ή την ανάγκη επιβολής διορθώσεων και τα αποτελέσματα των προηγούμενων επιθεωρήσεων για κάθε τμήμα της εταιρίας.

Ο ΥΔΠ μπορεί να προτείνει έκτακτη επιθεώρηση σε κάποιο τμήμα της εταιρείας, όταν κριθεί σκόπιμο.
Κατά την διάρκεια της επιθεώρησης υπάρχει επικοινωνία με το προσωπικό, εξετάζονται αρχεία και παρακολουθείται η εξέλιξη των εργασιών.
Μετά το τέλος της επιθεώρησης ο επιθεωρητής συνοψίζει στον επιθεωρούμενο τα θέματα που προέκυψαν και καταγράφει τα αποτελέσματα στην Έκθεση Επιθεώρησης.
Ο ΥΔΠ είναι υπεύθυνος για την παρακολούθηση της υλοποίησης των διορθωτικών ενεργειών, όπως αυτές έχουν τεκμηριωθεί σε έντυπο.
Τα αποτελέσματα των εσωτερικών επιθεωρήσεων αποτελούν εισερχόμενα στην ανασκόπηση της Διοίκησης.

3.8 Υλοποίηση προϊόντος

Σκοπός της παρούσας Διαδικασίας είναι να περιγράψει τη διαδικασία υλοποίησης των «προϊόντων» της εταιρείας που αφορά την παροχή υπηρεσιών στα εξής:

- Εσωτερική Οργάνωση των λειτουργιών των Επιχειρήσεων και Οργανισμών και Δημιουργία Δομημένων Συστημάτων Διοίκησης.
- Δημιουργία Δομημένων Συστημάτων Πληροφορικής προς υποστήριξη του αντίστοιχου Δομημένου Συστήματος Διοίκησης.
- Κατάρτιση Μελετών επί των Μηχανογραφικών αναγκών, Προσδιορισμός των Μηχανογραφικών μεγεθών και Σχεδιασμός του SOFTWARE.
- Δημιουργία Μηχανογραφικών Εφαρμογών προς κάλυψη του Δομημένου Συστήματος Πληροφορικής.
- Παροχή διαρκούς Τεχνικής Υποστήριξης όλων των ανωτέρω περιοχών.

Ο σχεδιασμός και η ανάπτυξη λογισμικού για φορείς όπως τα νοσοκομεία απαιτεί μια σειρά διαδικασιών που διενεργούνται από το προσωπικό της εταιρίας. Η ανάλυση των απαιτήσεων του νέου λογισμικού γίνεται από την ομάδα ποιότητας και σε περίπτωση που αξιολογηθεί θετικά η ανάληψη του έργου , το επόμενο βήμα πραγματοποιείται από τους προγραμματιστές της εταιρείας όπου γίνεται η περιγραφή του λογισμικού βάση τεχνικών προδιαγραφών και ο σχεδιασμός των

απαραίτητων εφαρμογών. Εφόσον ολοκληρωθεί και ελεγχθεί από τον διευθυντή παραγωγής ακολουθεί η υλοποίηση του προγράμματος που σημαίνει ότι προκύπτει ο κώδικας του προγράμματος ο οποίος ελέγχεται από τον επιβλέπων προγραμματιστή του τμήματος πριν γίνει ο τελικός έλεγχος από τον διευθυντή παραγωγής. Το αρχείο των παραπάνω διαδικασιών τηρείται ηλεκτρονικά.

Σε περίπτωση που δεν χρειαστεί η ανάπτυξη νέου λογισμικού , όπως και γίνεται στις περισσότερες των περιπτώσεων και η εταιρεία αναλάβει την οργάνωση και μηχανογράφηση κάποιου φορέα υπογράφεται η σχετική σύμβαση του έργου, στην οποία αναφέρονται το λογισμικό της εταιρείας, οι εφαρμογές και εκδόσεις του καθώς και καθορίζεται και η τεχνική τους υποστήριξη. Η υπογραφή της σύμβασης, η οποία ελέγχεται από τις αρμόδιες Υπηρεσίες της Αναθέτουσας Αρχής, ουσιαστικά επικυρώνει τον έλεγχο του προγράμματος , την εφαρμογή του και την ορθή λειτουργία του.

Η διαδικασία εγκατάστασης ενός προγράμματος, έχει ως αφετηρία την επίσκεψη από εκπαιδευμένο προσωπικό της εταιρείας στο φορέα, με σκοπό την εγκατάσταση των ολοκληρωμένων πληροφοριακών συστημάτων της εταιρίας. (π.χ. **‘HOSPITAL-2003’)**

Επόμενο βήμα μετά την εγκατάσταση είναι η παραμετροποίηση που σημαίνει η προσαρμογή και η ρύθμιση των παραμέτρων του συστήματος στις απαιτήσεις του νοσοκομείου. Την παραμετροποίηση ακολουθεί η μετάπτωση δεδομένων κατά την οποία εισέρχονται στο σύστημα στοιχεία και πληροφορίες που αφορούν το νοσοκομείο και ενημερώνουν το σύστημα.

Παράλληλα με την εγκατάσταση του συστήματος γίνεται και η επιτόπια εκπαίδευση (on site) με τις βασικές λειτουργίες των προγραμμάτων στους χρήστες του νοσοκομείου και τηρείται αρχείο. Η εκπαίδευση των χρηστών συνεχίζεται τηλεφωνικά ή επιτόπια σε θέματα που αφορούν την καθημερινή χρήση των εφαρμογών.

Ο έλεγχος υλοποίησης του προϊόντος γίνεται με δύο τρόπους . Πριν την παράδοση του συστήματος στον πελάτη, ο υπεύθυνος παραγωγής, κάνει ένα τυπικό έλεγχο για την παράδοση του προγράμματος και τη λειτουργία των εφαρμογών.

Κατά την παράδοση, το τμήμα πληροφορικής του νοσοκομείου ελέγχει τις εφαρμογές του προγράμματος και δίνει την έγκρισή του επιβεβαιώνοντας την ορθή του εγκατάσταση στο σύστημα του νοσοκομείου και συμπληρώνεται έντυπο. Για την εκπαίδευση του προσωπικού του πελάτη χρησιμοποιείται το κατάλληλο έντυπο.

Ο επαληθευτικός έλεγχος καλής λειτουργίας των προγραμμάτων πραγματοποιείται προγραμματισμένα μέσω εντύπου με υπεύθυνους τους επικεφαλείς των τμημάτων. Σε περίπτωση που διαπιστωθεί κάποιο συνεχιζόμενο πρόβλημα ακολουθείται η διαδικασία ελέγχου μη συμμορφώσεων – διορθωτικές και προληπτικές ενέργειες.

Με την ολοκλήρωση και την παράδοση του έργου στο φορέα υπάρχει η δυνατότητα υπογραφής σύμβασης τεχνικής υποστήριξης του λογισμικού (SLA, Service Level Agreement)

Σε περίπτωση που επέλθουν αλλαγές στο θεσμικό και κανονιστικό πλαίσιο της λειτουργίας του πελάτη, η εταιρεία δύναται να προχωρήσει στην υλοποίηση αυτών των αλλαγών ανάλογα και με το συμβόλαιο τεχνικής υποστήριξης που έχει με τον πελάτη.

Στα πλαίσια της σύμβασης της τεχνικής υποστήριξης η εταιρεία δύναται να προβεί σε βελτιώσεις ή αναβαθμίσεις που αιτείται ο πελάτης ή σε εγκατάσταση νέων εκδόσεων/ αναβαθμίσεων του λογισμικού της. Η κάθε συμφωνία με το φορέα περιγράφει χρόνους παράδοσης λογισμικού και χρόνους ανταπόκρισης-αποκατάστασης σε ανώμαλες λειτουργίες (bugs) .Σε περίπτωση που δεν αναφέρονται σχετικά χρόνοι ανταπόκρισης-παράδοσης, η εταιρεία έχει θέσει τους εξής πίνακες:

Πίνακας 2 "Χρόνοι ανταπόκρισης εταιρίας"

ΠΙΝΑΚΑΣ ΧΡΟΝΩΝ ΑΝΤΑΠΟΚΡΙΣΗΣ	
ΚΡΙΣΙΜΟΤΗΤΑ	**ΧΡΟΝΟΣ ΑΝΤΑΠΟΚΡΙΣΗΣ**
ΕΠΕΙΓΟΝ	4 ώρες εάν το αίτημα δοθεί έως τις 13:00 αλλιώς επόμενη εργάσιμη ημέρα
ΥΨΗΛΗ	1 εργάσιμη ημέρα
ΜΕΤΡΙΑ	2 εργάσιμες ημέρες
ΧΑΜΗΛΗ	3 εργάσιμες ημέρες

Και ακολουθούν μετά από την ημέρα ανταπόκρισης οι χρόνοι αποκατάστασης :

Πίνακας 3 "Χρόνοι αποκατάστασης εταιρίας"

ΠΙΝΑΚΑΣ ΧΡΟΝΩΝ ΑΠΟΚΑΤΑΣΤΑΣΗΣ	
ΚΡΙΣΙΜΟΤΗΤΑ	**ΧΡΟΝΟΣ ΑΠΟΚΑΤΑΣΤΑΣΗΣ**
ΕΠΕΙΓΟΝ	5 εργάσιμες ημέρες
ΥΨΗΛΗ	5 εργάσιμες ημέρες
ΜΕΤΡΙΑ	10 εργάσιμες ημέρες
ΧΑΜΗΛΗ	10 εργάσιμες ημέρες

3.9 Σχεδιασμός νέου προϊόντος

Σκοπός της διαδικασίας αυτής είναι ο προσδιορισμός του τρόπου σχεδιασμού και μελέτης των νέων προϊόντων, που η εταιρεία θέλει να παράγει.

Ως «προϊόν» ορίζεται η υπηρεσία της εταιρίας να παρέχει και να υποστηρίζει την εφαρμογή συγκεκριμένων προγραμμάτων – λογισμικού (software) που καλύπτει τις εκάστοτε ανάγκες των πελατών της.

- **Δεδομένα σχεδιασμού**

Μόλις η εταιρία κρίνει ότι κάποιο «προϊόν» έχει εμπορικό ενδιαφέρον (εύρος πωλήσεων, μείωση κόστους κ.λ.π.), συγκαλείται συμβούλιο της Ομάδας Ποιότητας.

Η μελέτη ξεκινά με την αρχική περιγραφή του «προϊόντος». Αμέσως μετά γίνεται διερεύνηση για τους κανονισμούς, νομοθεσία, πρότυπα κ.λ.π. που μπορεί να αφορούν το «προϊόν» αυτό.

Οι απαιτήσεις αυτές μετατρέπονται σε τεχνικές προδιαγραφές. Στη συνέχεια ελέγχονται οι προδιαγραφές αυτές ώστε να εξασφαλιστεί η δυνατότητα πραγματοποίησης της μελέτης.

Στη συνέχεια το έργο έρευνας και ανάπτυξης του προϊόντος καταγράφεται και αναλύεται σε επί μέρους φάσεις μελέτης και φάσεις ελέγχων. Για κάθε φάση προσδιορίζεται αρχικά κάποιος χρόνος υλοποίησης καθώς επίσης και οι απασχολούμενοι σ’ αυτή, με τις υπευθυνότητες τους. Η παρακολούθηση της

μελέτης γίνεται με καταγραφή της στο έντυπο προγραμματισμός σχεδιασμού προϊόντος.

Σε περίπτωση που η μελέτη ως προς κάποιο τμήμα της ανατεθεί σε εξωτερικό συνεργάτη, αυτός πρέπει να έχει αξιολογηθεί ότι διαθέτει την απαραίτητη τεχνογνωσία και τον κατάλληλο εξοπλισμό γιά να αναλάβει τη μελέτη. Πριν την ανάθεση συντάσσεται ιδιωτικό συμφωνητικό, στο οποίο περιγράφονται οι συμβατικές υποχρεώσεις του συνεργάτη, οι προδιαγραφές της μελέτης που θα αναλάβει και όποιες άλλες λεπτομέρειες κρίνονται απαραίτητες.

- **Αποτελέσματα σχεδιασμού**

Το «προϊόν» παρακολουθείται ως προς την πορεία υλοποίησής της έρευνας και ανάπτυξής του και ελέγχεται περιοδικά για να διαπιστωθεί:

- η συμφωνία με τα δεδομένα σχεδιασμού (προδιαγεγραμμένες απαιτήσεις)
- η συνέπεια του αποτελέσματος σχεδιασμού με την προηγηθείσα καταγραφή και ανάλυση

Κατά το σχεδιασμό τηρούνται απολογιστικά στοιχεία, τα οποία είτε παρακολουθούνται από το εργαλείο GitLab που χρησιμοποιεί η εταιρία, είτε εναλλακτικά συμπληρώνονται στο έντυπο Απολογισμού σχεδιασμού.

- **Αλλαγές / Τροποποιήσεις σχεδιασμού**

Κατά το σχεδιασμό ενός «προϊόντος» μπορεί να απαιτηθούν αλλαγές και τροποποιήσεις. Οι αλλαγές αυτές μπορούν να προκύψουν ως αποτέλεσμα διορθωτικών / προληπτικών ενεργειών που αφορούν ήδη μελετημένο «προϊόν», αλλαγών σε πρότυπα, κανονισμούς, προδιαγραφές που το διέπουν, αλλαγές στα δεδομένα της αγοράς ή ακόμα και ως αποτέλεσμα της εμπειρίας που στο μεταξύ έχει αποκτηθεί από τους μελετητές πάνω στο συγκεκριμένο «προϊόν».

Πριν την έναρξη της αλλαγής εκτιμάται τεχνικά και οικονομικά το εφικτό της αλλαγής. Αν η αλλαγή μπορεί να πραγματοποιηθεί, τότε γίνεται μία πρώτη εκτίμηση των χρονικών και κοστολογικών επιδράσεων της αλλαγής και εφόσον αποφασιστεί η συνέχιση της μελέτης, γίνονται οι απαραίτητες τροποποιήσεις, τόσο στη σχεδίαση όσο και στον προγραμματισμό.

Ιδιαίτερη βαρύτητα κατά τις αλλαγές στο σχεδιασμό δίδεται προκειμένου να αναγνωριστούν επιδράσεις της αλλαγής σε δεδομένα και στοιχεία του «προϊόντος» που ήδη έχουν γίνει αποδεκτά σε προηγούμενες φάσεις του σχεδιασμού.

Οι αλλαγές είτε παρακολουθούνται από το εργαλείο GitLab που χρησιμοποιεί η εταιρία, είτε εναλλακτικά καταχωρούνται στο φάκελο της μελέτης και οι εμπλεκόμενοι ενημερώνονται σύμφωνα με τη σχετική διαδικασία ελέγχου εγγράφων.

- **Ανασκόπηση σχεδιασμού**

Με την ανασκόπηση του σχεδιασμού διασφαλίζουμε ότι:

- Ο σχεδιασμός ακολουθεί τις προδιαγραφές που έχουν τεθεί
- Εξασφαλίζεται η δυνατότητα υλοποίησης του «προϊόντος», με βάση τους χρονικούς και οικονομικούς περιορισμούς
- Έχουν εντοπιστεί τα σημεία εκείνα του «προϊόντος» που είναι κρίσιμα γιά τη σωστή λειτουργία και απόδοσή του.

Η ανασκόπηση του σχεδιασμού μπορεί να γίνει αρχικά, ώστε να βεβαιωθούμε ότι όλα τα στοιχεία του σχεδιασμού έχουν ληφθεί υπόψη, αλλά και ενδιάμεσα, σε περίπτωση που υπάρξουν αλλαγές στα δεδομένα σχεδιασμού ή άλλοι λόγοι.

Η ανασκόπηση του σχεδιασμού γίνεται πάντα και στο τέλος του σχεδιασμού για να επιβεβαιωθεί η ορθότητα της μελέτης καθώς και η συμφωνία του πελάτη / αγοράς / δεδομένων σχεδιασμού με αυτήν.

Στην τελική ανασκόπηση συμμετέχουν όλα τα μέλη της Ομάδας Ποιότητας.

Κατά την ανασκόπηση του σχεδιασμού τηρούνται τα σχετικά στοιχεία, τα οποία είτε παρακολουθούνται από το εργαλείο GitLab που χρησιμοποιεί η εταιρία, είτε εναλλακτικά συμπληρώνονται στο έντυπο Ανασκόπησης σχεδιασμού.

- **Επαλήθευση του σχεδιασμού και της ανάπτυξης**

Με την ολοκλήρωση του σχεδιασμού (παραγωγή δοκιμαστικών εφαρμογών) ακολουθεί η επαλήθευση των αποτελεσμάτων με τα απαιτούμενα κατά τον προγραμματισμό του σχεδιασμού αντίστοιχου προϊόντος. Η επαλήθευση γίνεται από την Ομάδα Ποιότητας, η οποία και προγραμμάτισε τον σχεδιασμό και ανάπτυξη νέου προϊόντος. Συγκρίνονται τα εισερχόμενα δεδομένα με τα πραγματικά αποτελέσματα (λειτουργία προγράμματος και εφαρμογών, χρηστικότητα προγράμματος, ενημέρωση προγράμματος, εκπαίδευση προσωπικού κλπ). Τα αποτελέσματα τεκμηριώνονται και αρχειοθετούνται όπως και αυτά της ανασκόπησης.

- **Επικύρωση του σχεδιασμού και της ανάπτυξης**

Η επικύρωση όλων των διαδικασιών σχεδιασμού και ανάπτυξης γίνεται από την Διοίκηση της εταιρίας με έκδοση όλων των απαραίτητων εγγράφων (διαγράμματα ροής, τεχνικές προδιαγραφές, οδηγίες εργασίας κλπ) για το νέο προϊόν, το οποίο ενσωματώνεται στο σύστημα ποιότητας της εταιρείας.

- **Έλεγχος των αλλαγών του σχεδιασμού και της ανάπτυξης**

Σε περίπτωση που κατά την επαλήθευση του σχεδιασμού και της ανάπτυξης βρεθεί απόκλιση από τις προδιαγεγραμμένες απαιτήσεις για το νέο προϊόν, τότε γίνονται αλλαγές στα ανάλογα στάδια. Καταγράφονται τα δεδομένα αλλαγών στα πρόχειρα διαγράμματα και τεχνικές προδιαγραφές. Η κάθε αλλαγή είτε παρακολουθείται από το εργαλείο GitLab που χρησιμοποιεί η εταιρία, είτε εναλλακτικά παίρνει ένα νέο αριθμό δοκιμής, τεκμηριώνεται η ημερομηνία αλλαγής, υπογράφεται από τον υπεύθυνο εφαρμογής και αρχειοθετείται.

3.10 Ανάλυση δεδομένων & συνεχής βελτίωση

Σκοπός της παρούσας Διαδικασίας είναι να περιγραφεί ο τρόπος με τον οποίο διασφαλίζεται η βελτίωση της αποτελεσματικότητας του Συστήματος Διαχείρισης Ποιότητας.

Η εταιρία για την αξιολόγηση του συστήματος χρησιμοποιεί κάποιους δείκτες για την ποιότητα.

- **Επιλογή Δεικτών**
  - Η Ομάδα Ποιότητας επιλέγει τους δείκτες, εκείνους που εκφράζουν το πεδίο δραστηριότητας και το σύνολο των διεργασιών της εταιρίας, και είναι δυνατόν να παρακολουθούνται.
- **Ενημέρωση Δεικτών**
  - Ο κάθε δείκτης ενημερώνεται στην συχνότητα που ορίζεται από τον Υπεύθυνο Διαχείρισης Ποιότητας.
  - Ο ΥΔΠ είναι υπεύθυνος σύνταξης της αναφοράς δεικτών συνεχούς βελτίωσης.
- **Θέσπιση στόχων**
  - Η Ομάδα Ποιότητας ορίζει τον στόχο για τον κάθε δείκτη. Ο στόχος μπορεί να είναι μεσοπρόθεσμος ή μακροπρόθεσμος.

- Οι στόχοι περιγράφονται στην αναφορά δεικτών συνεχούς βελτίωσης Ε-10-01 και παράλληλα περιγράφεται και ο τρόπος επίτευξης τους, καθώς και τα άτομα που συμμετέχουν στην επίτευξη τους.

Τα στοιχεία που λαμβάνονται αναλύονται και τα συμπεράσματα της ανάλυσης αποτελούν εισερχόμενα στην Ανασκόπηση της Διοίκησης.

3.11.1 Ανάλυση διακινδύνευσης & ενδιαφερόμενα μέρη

Σκοπός της διαδικασίας είναι η περιγραφή των υπευθυνοτήτων, των διαδικασιών λειτουργίας και των εντύπων που χρησιμοποιεί η εταιρεία για τον σχεδιασμό διαχείρισης της διακινδύνευσης αναφορικά με ζητήματα Ποιότητας.

Σε αυτή τη διαδικασία προσδιορίζονται τα στοιχεία των δραστηριοτήτων, των υπηρεσιών που αλληλεπιδρούν με το περιβάλλον (περιβαλλοντικές πλευρές-προγράμματα κλπ), καθώς και η διαδικασία προσδιορισμού κινδύνων και αξιολόγησης κινδύνων.

Ο προσδιορισμός και η αξιολόγηση της διακινδύνευσης αφορά:

- το σύνολο των τρεχουσών και δυνητικά μελλοντικών δραστηριοτήτων στις εγκαταστάσεις της εταιρίας,
- το σύνολο των στοιχείων επί των οποίων η εταιρία μπορεί να ασκεί άμεσο ή έμμεσο έλεγχο,
- τις φυσιολογικές, μη φυσιολογικές καταστάσεις και τις καταστάσεις εκτάκτου ανάγκης.

Επίσης σκοπός της διαδικασίας είναι να περιγράψει τα ενδιαφερόμενα μέρη και τις απαιτήσεις τους που σχετίζονται με το Σύστημα Ποιότητας

- **Αναγνώριση Διακινδύνευσης Ποιότητας**

Για την αναγνώριση της διακινδύνευσης αναφορικά με την επίδραση στην Ποιότητα των παρεχόμενων προϊόντων, χρησιμοποιείται το έντυπο: Ανάλυση Διακινδύνευσης, χρησιμοποιώντας σύστημα αξιολόγησης δυο παραμέτρων. Ο τρόπος βαθμολόγησης και αξιολόγησης παρουσιάζεται σε επόμενη παράγραφο.

Πιο συγκεκριμένα στο εν λόγο έντυπο καταγράφονται όλες οι δραστηριότητες οι οποίες δύναται να επηρεάσουν την ποιότητα των παρεχόμενων προϊόντων και λαμβάνονται υπόψη όλα τα ενδιαφερόμενα μέρη.

- **Ανάλυση Διακινδύνευσης**

Για κάθε διακινδύνευση που έχει εντοπισθεί και καταγραφεί γίνεται ανάλυση των πιθανών επιπτώσεων που δύναται να επιφέρει. Για την ανάλυση των επιπτώσεων λαμβάνονται υπόψη όλα τα ενδιαφερόμενα μέρη και απαιτήσεις τους.

- **Αξιολόγηση Διακινδύνευσης**

Η αξιολόγηση κινδύνων είναι η διαδικασία προσδιορισμού, αξιολόγησης και εκτίμησης των επιπέδων διακινδύνευσης που ενέχει μια κατάσταση και ο καθορισμός ενός αποδεκτού επιπέδου κινδύνου, είτε αυτός αφορά ζήτημα ποιότητας, ασφάλειας ή και υγείας.

Κατά τη διενέργεια αξιολογήσεων κινδύνων αξιολογείται ο κίνδυνος που εντοπίζεται στο πλαίσιο μιας λειτουργίας. Το επίπεδο κινδύνου βαθμολογείται βάσει ορισμένων παραγόντων, ενώ για τους κινδύνους που παρουσιάζουν χαμηλή βαθμολογία (είτε κατά την αρχική αξιολόγηση είτε κατά την επαναξιολόγηση) δεν απαιτούνται κατά κανόνα ενέργειες ή μέτρα ελέγχου αλλά απαιτείται η παρακολούθησή τους.

Ως κρίσιμοι κίνδυνοι για κάθε παρακολουθούμενο άξονα διαχείρισης ορίζονται οι κίνδυνοι που τελικά αξιολογούνται ως Υψηλής Διακινδύνευσης.

Η αξιολόγηση της διακινδύνευσης γίνεται από τον ΥΔΠ, σε συνεργασία με όποιον κατά περίπτωση κρίνει απαραίτητο.

Για τον υπολογισμό της διακινδύνευσης λαμβάνεται υπόψη ο ακόλουθος τύπος:

ΔΙΑΚΙΝΔΥΝΕΥΣΗ = ΠΙΘΑΝΟΤΗΤΑ x ΣΟΒΑΡΟΤΗΤΑ

Η κλίμακα της πιθανότητας και σοβαρότητας παρατίθεται στους ακόλουθους πίνακες:

Πίνακας 4 "Κλίμακα της πιθανότητας εμφάνισης διακινδύνευσης"

ΠΙΘΑΝΟΤΗΤΑ		
Τιμή	**Επίπεδο**	**Ορισμός**
1	Απίθανο	0%-10%
2	Μάλλον απίθανο	11% - 35%

3	Πιθανό	36%-65%
4	Πολύ Πιθανό	65%-89%
5	Σίγουρο	90%-100%

Πίνακας 5 "Κλίμακα σοβαρότητας εμφανιζόμενης απειλής"

ΣΟΒΑΡΟΤΗΤΑ ΕΠΙΠΤΩΣΗΣ ΑΠΕΙΛΗΣ		
Τιμή	**Επίπεδο**	**Ορισμός**
1	Πολύ μικρής σημασίας	Υπάρχει επίπτωση αλλά δεν είναι άξια προβληματισμού και λήψης ιδιαιτέρων μέτρων
2	Ήσσονος σημασίας	Πλήρως αντιστρεπτή επίπτωση χωρίς καμία παραμένουσα επιβάρυνση
3	Σημαντική	Αντιστρεπτή επίπτωση με μικρό χρονικό διάστημα αποκατάστασης ή μικρού εύρους και χωρίς ή με μικρή παραμένουσα επιβάρυνση
4	Σοβαρή	Αντιστρεπτή επίπτωση, αλλά με μεγάλο χρονικό διάστημα αποκατάστασης ή μεγάλου εύρους και σοβαρή παραμένουσα επιβάρυνση
5	Πολύ σοβαρή	Με αντιστρεπτή επίπτωση

Πίνακας 6 "Κλίμακα σοβαρότητας εμφανιζόμενης ευκαιρίας"

ΣΟΒΑΡΟΤΗΤΑ ΕΠΙΠΤΩΣΗΣ ΕΥΚΑΙΡΙΑΣ		
Τιμή	**Επίπεδο**	**Ορισμός**
1	Πολύ μικρής σημασίας	Δεν υπάρχει καμία σχεδόν αξία από την εκμετάλλευση της ευκαιρίας
2	Ήσσονος σημασίας	Προσδίδεται μικρή αξία/ όφελος από την εκμετάλλευση της ευκαιρίας
3	Σημαντική	Υπάρχει αξία/ όφελος από την εκμετάλλευση της ευκαιρίας
4	Σοβαρή	Υπάρχει σημαντική αξία/όφελος από την εκμετάλλευση της ευκαιρίας
5	Πολύ σοβαρή	Υπάρχει ιδιαίτερα σημαντική αξία/όφελος από την εκμετάλλευση της ευκαιρίας

Από το γινόμενο των ανωτέρω παραμέτρων αξιολόγησης προκύπτει ο ακόλουθος πίνακας, με τέσσερις κατηγορίες κινδύνου.

Πίνακας 7 "Κατηγοριοποίηση και ερμηνεία Αξιολόγησης Διακινδύνευσης"

ΣΟΒΑΡΟΤΗΤΑ	ΠΙΘΑΝΟΤΗΤΑ				
	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

- **Διαχείριση Διακινδύνευσης**

Εφόσον καταγραφή η αξιολόγηση της διακινδύνευσης το επόμενο στάδιο είναι η επιλογή του τρόπου διαχείρισης της. Πιο συγκεκριμένα για την περίπτωση των απειλών οι επιλογές διαχείρισης τους είναι:

- Εξάλειψη
- Μείωση
- Αποφυγή
- Μεταφορά

ενώ για την περίπτωση των ευκαιριών οι επιλογές είναι:

- Εκμετάλλευση
- Συμμετοχή
- Ενίσχυση
- Αψήφηση

- **Προγράμματα Ενεργειών**

Το επόμενο στάδιο και αφού έχει επιλεγεί η στρατηγική διαχείρισης της διακινδύνευσης καθορίζονται τα προτεινόμενα μέτρα διαχείρισης, οι αρμόδιοι υλοποίησης και τα χρονικά περιθώρια. Με τον τρόπο αυτό προκύπτει ένα δυναμικό πρόγραμμα ενεργειών στο οποίο περιλαμβάνονται πτυχές διαχείρισης της διακινδύνευσης.

- **Αναθεώρηση Διακινδύνευσης-Προγραμμάτων Ενεργειών**

Η αναθεώρηση και επικαιροποίηση της διακινδύνευσης διενεργείται άμεσα σε ορισμένες περιπτώσεις, όπως:

- Η θέσπιση ή τροποποίηση νομοθετικών απαιτήσεων ή συμφωνιών.
- Η τροποποίηση επιχειρηματικών διαδικασιών και στοιχείων.
- Η μη συμμόρφωση ή αιτήματα για διορθωτικές ενέργειες.
- Η μεταβολή του χρησιμοποιούμενου εξοπλισμού
- Η χρήση νέων ουσιών, προϊόντων και/ή πρώτων υλών.
- Οι εσωτερικές και εξωτερικές επικοινωνίες.
- Η εμφάνιση συμβάντος

Ακόμα και στην περίπτωση που δεν συντρέχει κανένας από τους παραπάνω λόγους, το έντυπο Ανάλυση Διακινδύνευσης επανελέγχεται σε ετήσια βάση.

- **Ενδιαφερόμενα μέρη**

Στον παρακάτω πίνακα παρουσιάζονται τα ενδιαφερόμενα μέρη και η εμπλοκή τους με το εφαρμοζόμενο Σύστημα Διαχείρισης Ποιότητας

Πίνακας 8 "Ενδιαφερόμενα μέρη"

Ενδιαφερόμενα Μέρη	Προσδοκίες / Απαιτήσεις	Παρακολούθηση και Ανασκόπηση μέσω:
Πελάτες	Τιμή, αξιοπιστία προϊόντων και τεχνική υποστήριξη	Παρακολούθηση μέσω της διαδικασίας υλοποίηση προϊόντος Help desk/GLPI Αξιολόγηση μέσω των ερωτηματολογίων ικανοποίησης πελάτη Ανασκόπηση από τη Διοίκηση
Ανταγωνισμός / Εταιρείες του κλάδου	Ανταγωνιστικές τιμές / υπηρεσίες	Παρακολούθηση από συμβάσεις και συμμετοχές σε διαγωνισμούς (δημόσια έγγραφα).
Ιδιοκτήτες	Ανάπτυξη και κερδοφορία	Αξιολόγηση μέσω της διαδικασίας : Ανάλυση δεδομένων & συνεχής βελτίωση Ανασκόπηση από τη Διοίκηση

Υπάλληλοι	Προσωπική επαγγελματική ανάπτυξη και εργασιακή ασφάλεια	Παρακολούθηση και Αξιολόγηση μέσω της διαδικασίας Διαχείριση Προσωπικού - Εκπαίδευση
Προμηθευτές / Τράπεζες	Αγαστή συνεργασία, πληρωμή, ικανοποίηση συμφωνητικών.	Παρακολούθηση και Αξιολόγηση μέσω της διαδικασίας, Διαχείριση Προμηθειών – Προμηθευτών, Συμφωνητικά – συμβάσεις.
Επίσημοι Φορείς και Αρχές Φορέας πιστοποίησης Δημόσιο / Υπουργείο Υγείας)	Αγαστή συνεργασία και ικανοποίηση της Νομοθεσίας και των Απαιτήσεων / Συμβάσεων.	Παρακολούθηση και Αξιολόγηση κατά την ανασκόπηση Διαδικασία επικοινωνίας (κατάλογος εξωτερικών εγγράφων) Συμβάσεις

3.11.2 Διαδικασία εντοπισμού κινδύνων ασφάλειας πληροφοριών

Η Διαδικασία αυτή προδιαγράφει τον τρόπο:

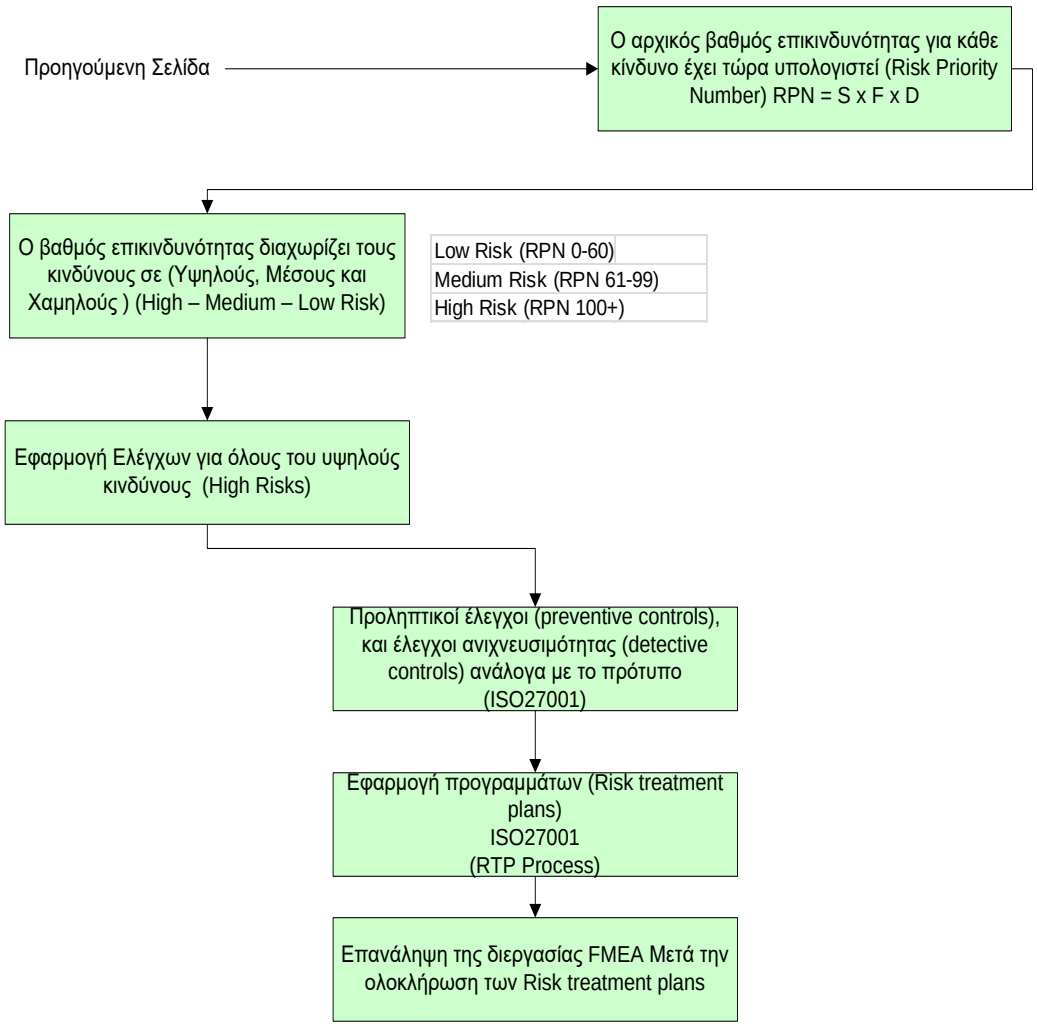
- εντοπισμού και αξιολόγησης των κινδύνων ασφάλειας πληροφοριών από τις δραστηριότητες της εταιρείας
- καθορισμού των επιπτώσεων των κινδύνων και των υφιστάμενων ελέγχων
- καθορισμού των προτεινόμενων ελέγχων

Παρακάτω παρουσιάζεται σχηματικά η όλη διαδικασία:

Effect	SEVERITY of Effect	Ranking
Catastrophic	Resource not available / Problem unknown	10
Extreme	Resource not available / Problem known and cannot be controlled	9
Very High	Resource not available / Problem known and can be controlled	8
High	Resource Available / Major violation of policies	7
Moderate	Resource Available / Major violations of process	6
Low	Resource Available / Major violations of procedures	5
Very Low	Resource Available / Minor violations of policies	4
Minor	Resource Available / Minor violations of process	3
Very Minor	Resource Available / Minor violations of procedures	2
None	No effect	1

PROBABILITY of Failure	Failure Prob	Ranking
Very High: Failure is almost inevitable	>1 in 2	10
	1 in 3	9
High: Repeated failures	1 in 8	8
	1 in 20	7
Moderate: Occasional failures	1 in 80	6
	1 in 400	5
	1 in 2,000	4
Low: Relatively few failures	1 in 15,000	3
	1 in 150,000	2
Remote: Failure is unlikely	<1 in 1,500,000	1

Detection	Likelihood of DETECTION	Ranking
Absolute Uncertainty	Control **cannot** prevent / detect potential cause/mechanism and subsequent failure mode	10
Very Remote	**Very remote** chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	9
Remote	**Remote** chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	8
Very Low	**Very low** chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	7
Low	**Low** chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	6
Moderate	**Moderate** chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	5
Moderately High	**Moderately High** chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	4
High	**High** chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	3
Very High	**Very high** chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	2
Almost Certain	Control **will** prevent / detect potential cause/mechanism and subsequent failure mode	1



Σχήμα 3 "Διαδικασία εντοπισμού κινδύνων ασφάλειας πληροφοριών"

3.12 Διαχείριση περιστατικών ασφαλείας

Σκοπός της διαδικασίας είναι να περιγράψει τον τρόπο διαχείρισης των Περιστατικών Ασφαλείας από το προσωπικό και τους συνεργάτες της εταιρείας. Στόχος είναι η εξασφάλιση του άμεσου εντοπισμού και απόκρισης στα Περιστατικά Ασφάλειας, καθώς και ο μετέπειτα προσδιορισμός των απαιτούμενων ενεργειών για την ελαχιστοποίηση των ενδεχόμενων αρνητικών συνεπειών για την εταιρεία.

Η Διαδικασία αυτή εφαρμόζεται σε όλη την Εταιρεία και αφορά όλα τα στελέχη και το προσωπικό της Εταιρείας.

Οι Διαχειριστές Δικτύου και Συστημάτων έχουν την ευθύνη για τη σχεδίαση, υλοποίηση και ανανέωση της τεχνικής λύσης, των διαδικασιών και όλων των απαραίτητων οδηγιών για τον εντοπισμό, περιορισμό και αντιμετώπιση των περιστατικών ασφάλειας

Ο Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών, συνεργάζεται με την Ανώτατη Διοίκηση, με σκοπό την ενημέρωσή της σχετικά με τα Περιστατικά Ασφάλειας και τη διευκόλυνση των διαχειριστικών αποφάσεων που πρέπει να ληφθούν. Επίσης, έχει συντονιστικό ρόλο κατά τη διάρκεια αντιμετώπισης των περιστατικών ασφάλειας.

- **Περιγραφή της διαδικασίας**

Ορισμοί:

Περιστατικό Ασφάλειας: Ως περιστατικό ασφάλειας μπορεί να θεωρηθεί οτιδήποτε μπορεί να προκαλέσει βλάβη στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πόρων, των υποδομών ή/και των πληροφοριών της εταιρείας. Ενδεικτικά, ένα περιστατικό ασφάλειας ενδέχεται να εμπίπτει σε μία από τις παρακάτω κατηγορίες.

- Μη εξουσιοδοτημένη πρόσβαση σε σταθμό εργασίας ή/και εξυπηρετητή ή/και οι σχετικές προσπάθειες
- Μη εξουσιοδοτημένη πρόσβαση σε εφαρμογή ή/και λογαριασμούς εφαρμογών, συμπεριλαμβανομένου του ηλεκτρονικού ταχυδρομείου ή παρόμοιων προσπαθειών
- Ιοί ή άλλα κακόβουλα λογισμικά (spyware, key logger etc) ή/και παρόμοιες προσπάθειες επίθεσης
- Παραλαβή ύποπτου ηλεκτρονικού μηνύματος και/ή επισυναπτόμενου σε αυτό αρχείου από μη έμπιστους αποστολείς ή/και παρόμοιων προσπαθειών
- Μη συνηθισμένες δραστηριότητες σε σταθμό εργασίας και/ή εξυπηρετητή ή εξαντλητική κατανάλωση πόρων (RAM, CPU) και/ή παρόμοια περιστατικά
- Καθυστέρηση ή άρνηση υπηρεσίας χωρίς πρότερη πληροφόρηση και/ή παρόμοια περιστατικά

- Άλλες δραστηριότητες που μπορούν πιθανόν να βλάψουν την εμπιστευτικότητα, ακεραιότητα και/ή διαθεσιμότητα της πληροφορίας (π.χ. κλοπή εξοπλισμού) ή/και παρόμοιες προσπάθειες.

- **Παρακολούθηση και ανίχνευση περιστατικών ασφάλειας**

Ο Διαχειριστής Δικτύου και ο Διαχειριστής Συστημάτων παρακολουθούν σε τακτική βάση όλους τους μηχανισμούς προστασίας και παρακολούθησης της υποδομής και προστασίας των πληροφοριών. Τέτοιοι μηχανισμοί μπορεί να είναι αρχεία καταγραφής, συστήματα πρόληψης επιθέσεων (βλ. Firewalls).

- **Εντοπισμός Περιστατικού Ασφάλειας**

Όταν κάποιος εντοπίσει μία απειλή, ενημερώνει μέσω email τον Υ.Δ.Α.Π. και τους Διαχειριστές Δικτύου Συστημάτων

Σε περίπτωση που η απειλή αφορά δεδομένα και πληροφορίες που βρίσκονται σε μη ηλεκτρονική μορφή, ο χρήστης θα πρέπει να επικοινωνεί απευθείας με τον Υ.Δ.Α.Π.

- **Παραλαβή αιτήματος**

Με την παραλαβή του αιτήματος, οι Διαχειριστές Δικτύου και Συστημάτων κατηγοριοποιούν την απειλή εξετάζοντας την κρισιμότητα της επίθεσης και των πληροφοριακών ή άλλων πόρων με τις οποίες αυτή σχετίζεται. Σύμφωνα με τις επιπτώσεις που ενδέχεται να επιφέρει, η απειλή μπορεί να χαρακτηριστεί ως Υψηλής, Μεσαίας ή Χαμηλής Κρισιμότητας.

Ο χαρακτηρισμός της κρισιμότητας της απειλής επικοινωνείται από τους Διαχειριστές Δικτύου και Συστημάτων στον Υ.Δ.Α.Π. μέσω email.

- **Ενέργειες Αντιμετώπισης**

Σύμφωνα με τη κρισιμότητα της απειλής, οι Διαχειριστές Δικτύου και Συστημάτων πραγματοποιούν ενέργειες που απαιτούνται για τον περιορισμό της απειλής. Οι αρχικές ενέργειες μπορεί να είναι:

- Απενεργοποίηση μερικών υπηρεσιών του συστήματος,
- Αλλαγή συνθηματικών και απενεργοποίηση λογαριασμών,
- Αποσύνδεση του προσβεβλημένου συστήματος από το υπόλοιπο δίκτυο,
- Προσωρινός τερματισμός της λειτουργίας του προσβεβλημένου συστήματος.

Σε κάθε περίπτωση, οι Διαχειριστές Δικτύου και Συστημάτων θα πρέπει να λαμβάνουν υπόψη τους τις απαιτήσεις διαθεσιμότητας, εμπιστευτικότητας και ακεραιότητας που σχετίζονται με το εκάστοτε σύστημα, και σε περίπτωση που υπάρχει πιθανότητα μη συμμόρφωσης με αυτές τις απαιτήσεις θα πρέπει να αιτούνται την έγκριση του Υ.Δ.Α.Π. πριν τη πραγματοποίηση ενεργειών.

- **Συλλογή Στοιχείων**

Μετά την πραγματοποίηση των αρχικών ενεργειών και σε περίπτωση που δεν έχει αντιμετωπιστεί πλήρως το περιστατικό, οι Διαχειριστές Δικτύου και Συστημάτων, υπό το συντονισμό του Υ.Δ.Α.Π. συγκεντρώνουν στοιχεία που θα τους βοηθήσουν στην αντιμετώπιση του περιστατικού και καθορίζουν τις επόμενες ενέργειες.

- **Περισσότερες Ενέργειες**

Όταν πρόκειται για κρίσιμη απειλή, η οποία έχει ευρέως διαδοθεί, τότε ο Υ.Δ.Α.Π. επικοινωνεί με τη Διοίκηση, προκειμένου να λάβει συγκατάθεση για απαιτούμενες περαιτέρω ενέργειες, όπως την απενεργοποίηση ενός συγκεκριμένου συστήματος ή υποδικτύου.

Σε όλη τη διαδικασία συλλέγονται ηλεκτρονικά στοιχεία, τα οποία και καταγράφονται έως ότου η Διοίκηση να αποφασίσει να ερευνήσει περαιτέρω το Περιστατικό Ασφάλειας και τις νομικές ή συμβατικές συνέπειες που αυτό ενδέχεται να έχει.

- **Ανασκόπηση Περιστατικών Ασφάλειας**

Μετά την αντιμετώπιση του περιστατικού, ο Υ.Δ.Α.Π. έχει τη δυνατότητα να αιτηθεί τη σύγκληση έκτακτης συνάντησης της Διοίκησης, σχετικά με το Περιστατικό. Η συνάντηση δεν πρέπει να γίνει αργότερα παρά μέσα σε τέσσερις (4) ημερολογιακές ημέρες από την εμφάνιση του Περιστατικού. Τα θέματα που θα συζητηθούν πρέπει να είναι τα παρακάτω:

- Εκτίμηση της ζημίας/επιπτώσεις,
- Ενέργειες που έγιναν κατά τη διάρκεια του Περιστατικού,
- Ενέργειες που πρέπει να γίνουν για την πλήρη εξάλειψη της ευπάθειας που προκάλεσε το περιστατικό ασφάλειας,
- Πολιτικές και διαδικασίες που πρέπει να ανανεωθούν,
- Περαιτέρω προληπτικές ενέργειες που ενδεχομένως να απαιτούνται.

3.13 Διαδικασία διαχείρισης αλλαγών

Ο σκοπός της διαδικασίας είναι να διασφαλιστεί ότι κάθε αλλαγή που πραγματοποιείται στο πληροφοριακό σύστημα της εταιρείας θα πραγματοποιείται με τρόπο ο οποίος διασφαλίζει την εύρυθμη λειτουργία των συστημάτων καθώς επίσης και την ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα των πληροφοριών που σχετίζονται με αυτές. Η Διαδικασία αυτή εφαρμόζεται σε όλη την Εταιρεία και αφορά όλα τα στελέχη και το προσωπικό της Εταιρείας.

Οι Διαχειριστές Δικτύου και Συστημάτων είναι υπεύθυνοι για την εξέταση των αιτημάτων αλλαγών και την υλοποίηση τους

Η ομάδα υλοποίησης κάθε αλλαγής είναι το προσωπικό στο οποίο οι Διαχειριστές Δικτύου και Συστημάτων αναθέτουν την πραγματοποίηση των αλλαγών, τόσο σε δοκιμαστικό, όσο και σε περιβάλλον παραγωγής.

Η διαδικασία αυτή αφορά αλλαγές που πρέπει να γίνουν στις παρακάτω κατηγορίες πόρων:

- Υλικό,
- Λογισμικό / Εφαρμογές / Λειτουργικό Σύστημα (αλλαγές εκδόσεων / βελτιώσεις / εγκατάσταση λογισμικού επιδιορθώσεις κ.λ.π.),
- Βάσεις Δεδομένων,
- Δικτυακός εξοπλισμός,
- Τηλεφωνία.

Οι αλλαγές μπορεί να αφορούν: εγκατάσταση, απεγκατάσταση ή αλλαγές σε ρυθμίσεις και τοποθεσία του εξοπλισμού. Επιπλέον, η Διαδικασία εφαρμόζεται στις περιπτώσεις που εντοπίζεται ότι υπάρχουν διαθέσιμες αναβαθμίσεις λογισμικού ή επιδιορθώσεις λογισμικού (patches) για συστήματα της εταιρείας.

- **Ανάγκη για Αλλαγή**

Η διαδικασία τίθεται σε εφαρμογή όταν υπάρξει ανάγκη για αλλαγή σε έναν από τους πόρους της πιο πάνω παραγράφου. Η ανάγκη προκύπτει μετά από αίτηση των Διαχειριστών Δικτύου και Συστημάτων ενός πόρου ή κάποιου χρήστη του πόρου.

- **Αίτηση Αλλαγής**

Ο αιτών την αλλαγή στέλνει e-mail στους Διαχειριστές Δικτύου και Συστημάτων στο οποίο περιλαμβάνονται κατ’ ελάχιστον οι παρακάτω πληροφορίες:

- Σύστημα, πληροφορία ή εξοπλισμός τον οποίο αφορά η αλλαγή
- Κρισιμότητα αλλαγής (Minor / Major / Emergency / Patch)
- Ημερομηνία αίτησης αλλαγής
- Αιτιολόγηση αλλαγής

- **Αξιολόγηση Αίτησης**

Οι Διαχειριστές Δικτύου και Συστημάτων εξετάζουν το e-mail του αιτούντος και αξιολογούν την περιγραφόμενη αλλαγή ως προς την αναγκαιότητα πραγματοποίησής της, την κρισιμότητά της, τις επιπτώσεις που μπορεί να επιφέρει η πραγματοποίηση ή μη πραγματοποίηση της και καθορίζει την προτεραιότητα διενέργειας της αλλαγής και ορίζει την καταληκτική ημερομηνία διεκπεραίωσης της.

Στην περίπτωση που η αίτηση αφορά εξοπλισμό ή συστήματα τα οποία σχετίζονται ή επηρεάζουν ευαίσθητη ή/και κρίσιμη πληροφορία, οι Διαχειριστές Δικτύου και Συστημάτων στέλνουν το e-mail με την «Αίτηση Αλλαγής» .

- **Πραγματοποίηση Αλλαγής**

Η αλλαγή πραγματοποιείται από την ομάδα υλοποίησης που ορίζεται από τους Διαχειριστές Δικτύου και Συστημάτων και στη συνέχεια ελέγχεται η επιτυχία της.

Εάν η αλλαγή δεν έγινε επιτυχημένα γίνεται χρήση αντιγράφων ασφαλείας για την επαναφορά των συστημάτων, εφόσον κριθεί απαραίτητο και εντοπίζεται και καταγράφεται η αιτία της αστοχίας της αλλαγής και οι εργασίες πραγματοποίησης της αλλαγής σταματούν μέχρι να δοθεί ανάλογη έγκριση από τον Επιβλέπων Προγραμματιστή.

- **Ολοκλήρωση Αλλαγής**

Οι Διαχειριστές Δικτύου και Συστημάτων αναλαμβάνουν την αρχειοθέτηση του mail «Αίτηση Αλλαγής». Οι επιτυχημένες αλλαγές, καθώς και οι αιτίες για την μη ορθή πραγματοποίηση αλλαγών, χρησιμοποιούνται ως αποκτηθείσα γνώση σε πιθανές μελλοντικές αλλαγές.

3.14 Διαδικασία διαχείρισης πρόσβασης

Σκοπός της διαδικασίας είναι να διασφαλιστεί ότι η διαχείριση των λογαριασμών των χρηστών γίνεται με ασφαλή και δομημένο τρόπο και ότι η πρόσβαση στις

πληροφορίες και τα συστήματα της εταιρείας γίνεται με τρόπο ασφαλή ως προς την ακεραιότητα, την εμπιστευτικότητα και την διαθεσιμότητα αυτών.

Για το σκοπό αυτόν η παρούσα διαδικασία ορίζει τον τρόπο με τον οποίο πραγματοποιείται η παροχή, η τροποποίηση και η κατάργηση των δικαιωμάτων στους χρήστες. Η περίπτωση της αλλαγής πρόσβασης αφορά τις περιπτώσεις που κάποιος υπάλληλος της εταιρείας είτε αλλάζει θέση, είτε τμήμα, είτε αποκτά έναν καινούργιο ρόλο.

Η Διαδικασία αυτή εφαρμόζεται σε όλη την Εταιρεία και αφορά όλα τα στελέχη και το προσωπικό της Εταιρείας.

Οι Διαχειριστές Δικτύου και Συστημάτων έχουν την ευθύνη ολοκλήρωσης των τεχνικών ρυθμίσεων που απαιτούνται για τη παροχή πρόσβασης, όπως επίσης να διεκπεραιώνουν τυχόν αιτήματα παροχής επιπλέον προσβάσεων.

Ο Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών, έχει την ευθύνη εξέτασης αιτημάτων παροχής επιπλέον προσβάσεων.

Οι Διαχειριστές Δικτύου και Συστημάτων, έχουν την ευθύνη παραλαβής αιτημάτων διαχείρισης πρόσβασης και διεκπεραίωσης τους.

Ορισμοί:

Πρόσβαση: ένα σύνολο δικαιωμάτων που παρέχουν στο χρήστη πρόσβαση σε ηλεκτρονικούς πόρους, χώρους και πληροφορίες της εταιρίας.

- **Έλεγχος Προσβασιμότητας στο δίκτυο της Εταιρείας**

Η πρόσβαση στο εσωτερικό δίκτυο της εταιρείας γίνεται κατά τέτοιο τρόπο, ώστε να εξασφαλίζεται η ασφαλέστερη δυνατή πρόσβαση σε αυτό με χρήση μηχανισμών ταυτοποίησης και αυθεντικοποίησης του χρήστη που προσπαθεί να εισέλθει σε αυτό. Ειδικότερα έχουν αξιοποιηθεί υπάρχοντες αλλά έχουν δημιουργηθεί και νέοι αυτοματοποιημένοι μηχανισμοί οι οποίοι ελέγχουν και αναλόγως, επιτρέπουν η απορρίπτουν την πρόσβαση στο εταιρικό Intranet. Ενδεικτικά :

- Ύπαρξη Εταιρικού Domain (με χρήση Domain Controller) για ταυτοποίηση και παρακολούθηση (Monitoring & Monitoring). Δυνατότητα ορισμού χρηστών και Ομάδων

- Τήρηση Active Directory για συνολική διαχείριση των υπολογιστών μελών του Domain
- Δυνατότητα ορισμού δικαιωμάτων πρόσβασης με χρήση των παραπάνω (Ποιος έχει πρόσβαση που)
- Δυνατότητα ορισμού πολιτικών και δικαιωμάτων σε επίπεδο ομάδων ανάλογα με τη φύση της εργασία που επιτελεί ο κάθε χρήστης
- Δυνατότητα ορισμού προσωπικού δικτυακού χώρου αλλά και ομαδικού (χώρου) για αυτοματοποίηση των εργασιών λήψης αντιγράφων ασφαλείας σε προσωπικό επίπεδο (domain user) αλλά και συνολική πολιτική ασφαλείας από εξουσιοδοτημένο χρήστη ο οποίος είναι υπεύθυνος με την λήψη και τήρηση αυτών (Διαχειριστές Δικτύου και Συστημάτων).

- **Παροχή Πρόσβασης σε Εργαζόμενο**
  - Έγκριση της Διοίκησης – υπογραφή σύμβασης εχεμύθειας – εμπιστευτικότητας
  - Δημιουργία νέου χρήστη στο Domain
  - Προστίθεται σε ομάδα με συγκεκριμένα δικαιώματα ανάλογα με το αντικείμενο εργασίας.
  - Δημιουργείται προσωπικός χώρος στο Domain
  - Αυτόματα γίνεται μέλος στο Back up της ομάδας
  - Του αποδίδεται κωδικός πρόσβασης με βάση την σχετική διαδικασία

Σε περίπτωση που ένας χρήστης χρειάζεται επιπλέον προσβάσεις για να επιτελέσει λειτουργίες που του έχουν ανατεθεί, μπορεί να αποστείλει απευθείας στους διαχειριστές δικτύου και συστημάτων email αιτήματος παροχής πρόσβασης ή επιπλέον χώρου.

- **Διακοπή Πρόσβασης σε Εργαζόμενο λόγω αλλαγής θέση ή αποχώρησης**
  - Εντολή της Διοίκησης
  - Κατάργηση χρήστη από το Domain
  - Τήρηση αντιγράφου Back up των αρχείων του στον Server
  - Κατάργηση των σχετικών κωδικών πρόσβασης

3.15 Διαδικασία λήψης και ανάκτησης δεδομένων ασφαλείας

Ο σκοπός της Διαδικασίας αυτής είναι να διασφαλίσει ότι δημιουργούνται αντίγραφα ασφάλειας των συστημάτων, των πληροφοριών και των δεδομένων της εταιρείας με τρόπο ο οποίος εξασφαλίζει τη διαθεσιμότητα τους, την ακεραιότητα τους και την εμπιστευτικότητα τους. Η Διαδικασία αυτή εφαρμόζεται σε όλη την Εταιρεία και αφορά όλα τα στελέχη και το προσωπικό της Εταιρείας

Ο Επιβλέπων Προγραμματιστής είναι το πρόσωπο που έχει προσδιοριστεί από τη διοίκηση να έχει την ευθύνη για τη διατήρηση της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας του αγαθού. Ο Επιβλέπων Προγραμματιστής για τον οποίο δημιουργείται αντίγραφο ασφάλειας, είναι αυτός που μπορεί να εκκινήσει τη Διαδικασία Επαναφοράς Αντιγράφων Ασφάλειας, σύμφωνα με όσα αναφέρονται στην παρούσα.

Οι Διαχειριστές Δικτύου και Συστημάτων έχουν επιφορτιστεί με την αρμοδιότητα να δημιουργούν αντίγραφα ασφάλειας, σύμφωνα με την παρούσα Διαδικασία και την Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων και να τα επαναφέρουν οποτεδήποτε τους ζητηθεί, από τον Ιδιοκτήτη του πρωτεύοντος αρχείου για το οποίο έχει δημιουργηθεί αντίγραφο ασφάλειας.

Ορισμοί:

Αντίγραφα ασφάλειας: Τα αντίγραφα των ηλεκτρονικών αρχείων πληροφοριών που αφορούν οτιδήποτε έχει αξία για τον οργανισμό και χρησιμοποιούνται για την ανάκτηση των πρωτευόντων αρχείων, σε περίπτωση καταστροφής των τελευταίων

- **Διαδικασία Δημιουργίας Αντιγράφων Ασφάλειας**
  - Περιοδική δημιουργία αντιγράφων ασφάλειας. Η διαδικασία ξεκινάει από τους Διαχειριστές Δικτύου και Συστημάτων, οποτεδήποτε απαιτείται να δημιουργηθεί αντίγραφο ασφάλειας για κάποιον από τους εταιρικούς πόρους.
  - Έλεγχος και διόρθωση αιτίας που οδήγησε στη μη δημιουργία του αντιγράφου. Πρέπει να ελεγχθεί η αιτία που οδήγησε στην αποτυχημένη δημιουργία του αντιγράφου ασφάλειας και να διορθωθεί. Εάν πρόκειται για συστήματα, δεδομένα ή πληροφορίες που έχουν διαβαθμιστεί ως

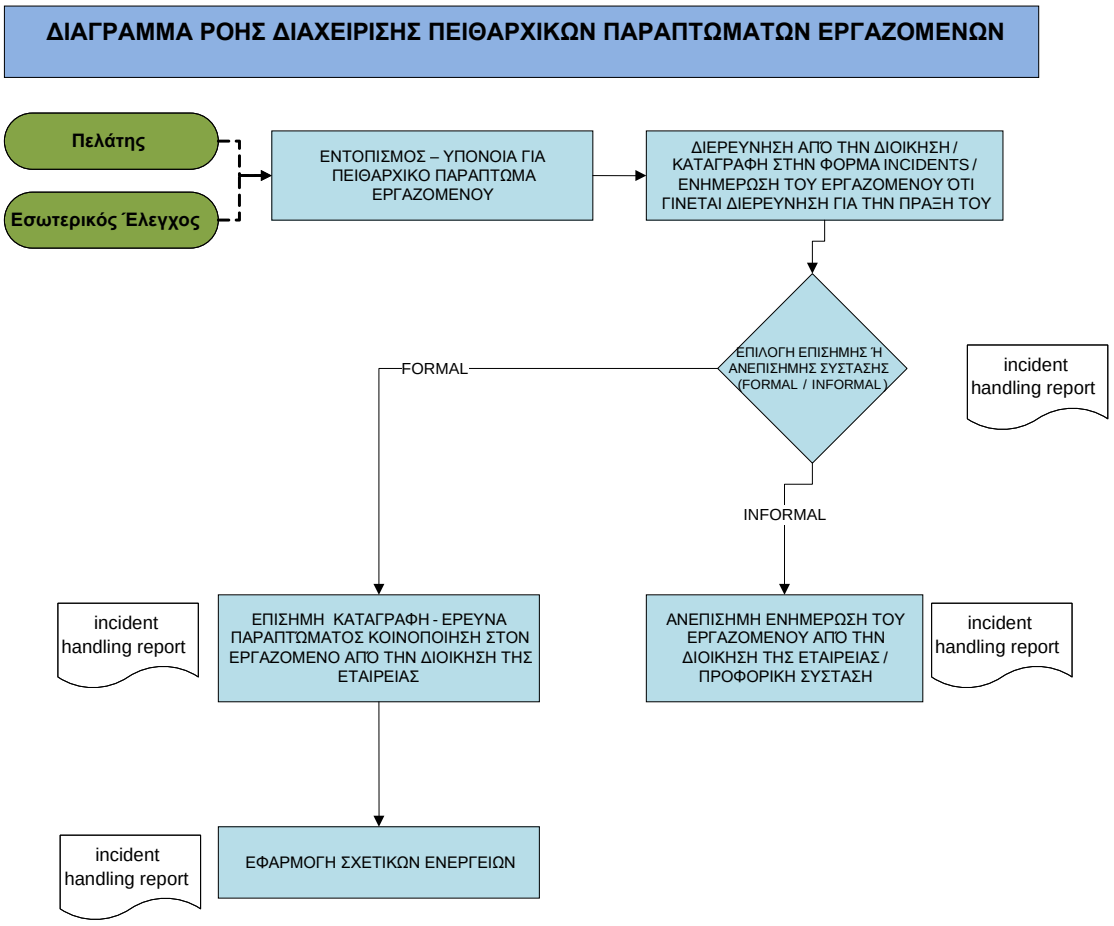
Εμπιστευτικά, τότε προγραμματίζεται άμεσα η επανάληψη της δημιουργίας αντιγράφου ασφάλειας, σε διαφορετική περίπτωση, η Διαδικασία της Δημιουργίας Αντιγράφου Ασφάλειας θα εκτελεστεί στην επόμενη προγραμματισμένη λήψη αντιγράφου.

- Φύλαξη των αντιγράφων ασφάλειας. Η φύλαξη των αντιγράφων ασφάλειας γίνεται με τρόπο που ανταποκρίνεται στις απαιτήσεις της εκάστοτε διαβάθμισης της πληροφορίας που περιέχουν, σύμφωνα με την Οδηγία Διαβάθμισης Δεδομένων ώστε να μη τίθενται σε κίνδυνο η ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα των πληροφοριών.

- **Διαδικασία επαναφοράς αντιγράφων ασφαλείας**
  - Απώλεια δεδομένων ή δοκιμή. Η διαδικασία ξεκινάει στις περιπτώσεις που υπάρχει απώλεια δεδομένων ή συστήματος. Επίσης εκτελείται από Επιβλέποντες Προγραμματιστές για δοκιμαστικούς λόγους.
  - Αίτημα επαναφοράς αντιγράφου ασφάλειας με αποστολή e-mail. Για την ανάκτηση συστήματος, εφαρμογής ή πληροφορίας, ένας χρήστης πρέπει να αποστείλει μία αίτημα επαναφοράς αντιγράφου ασφάλειας μέσω e-mail στους Διαχειριστές Δικτύου και Συστημάτων και στον Επιβλέπων Προγραμματιστή της συγκεκριμένης εφαρμογής ή της συγκεκριμένης πληροφορίας.
  - Έγκριση Αίτησης. Οι Διαχειριστές Δικτύου και Συστημάτων αξιολογούν την αίτηση προκειμένου να την εγκρίνουν ή να την απορρίψουν και στην περίπτωση που ανακτώνται εμπιστευτικές πληροφορίες απαιτείται επιπρόσθετα η έγκριση του Υ.Δ.Α.Π..
  - Επαναφορά αντιγράφου ασφάλειας. Εφόσον η αίτηση εγκριθεί υλοποιείται η επαναφορά.

3.16 Πειθαρχική διαδικασία (Disciplinary process)

Σχηματική παράσταση της πειθαρχικής διαδικασίας (Disciplinary process)



Σχήμα 4 "Πειθαρχική Διαδικασία"

3.17 Διαδικασία απρόσκοπτης – παραγωγικής λειτουργίας

Ο σκοπός της Διαδικασίας αυτής είναι να διασφαλίσει ότι τηρείται η απρόσκοπτη λειτουργία της εταιρείας σε περίπτωση εκτάκτων αναγκών – βλαβών υλικοτεχνικών υποδομών. Η Διαδικασία αυτή εφαρμόζεται σε όλη την Εταιρεία και αφορά όλα τα στελέχη και το προσωπικό της Εταιρείας.

Ο Επιβλέπων Προγραμματιστής είναι το πρόσωπο που έχει προσδιοριστεί από τη διοίκηση να έχει την ευθύνη για τη διατήρηση της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας του αγαθού. Ο Επιβλέπων Προγραμματιστής για τον οποίο δημιουργείται αντίγραφο ασφάλειας, είναι αυτός που μπορεί να

εκκινήσει τη Διαδικασία Επαναφοράς Αντιγράφων Ασφάλειας, σύμφωνα με όσα αναφέρονται στην παρούσα.

Οι Διαχειριστές Δικτύου και Συστημάτων έχουν επιφορτιστεί με την αρμοδιότητα να δημιουργούν αντίγραφα ασφάλειας, σύμφωνα με την παρούσα Διαδικασία και την Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων και να τα επαναφέρουν οποτεδήποτε τους ζητηθεί, από τον Ιδιοκτήτη του πρωτεύοντος αρχείου για το οποίο έχει δημιουργηθεί αντίγραφο ασφάλειας.

Σε επίπεδο τήρησης αντιγράφων ασφαλείας έχει ληφθεί μέριμνα έτσι ώστε να μην επηρεαστεί η εύρυθμη και απρόσκοπτη λειτουργία της εταιρίας, ακόμη και από βλάβες που πιθανόν να παρουσιαστούν σε σταθμούς εργασίας αλλά και σε επίπεδο υποδομών και προσβασιμότητας.

Ειδικότερα:

- **Διαχείριση Πρόσβασης στο εσωτερικό δίκτυο της εταιρίας**
  - ΄Υπαρξη Δευτερεύοντος Domain Controller ο οποίος αναλαμβάνει σε περίπτωση βλάβης του Πρωτεύοντος (αρχικού). Οι δύο Controllers συγχρονίζονται αυτόματα και όποια αλλαγή γίνει σε κάποιον από τους δύο ενημερώνει σε πραγματικό χρόνο τον άλλο. (Failover)
  - Μέριμνα για διαθεσιμότητα και ανοχή σε σφάλματα και αστοχία υλικού. Ο κάθε εξυπηρετητής και Domain Controller, έχει τη δυνατότητα ανοχής σε περίπτωση αστοχίας ή σφάλματος.

Ενδεικτικά αναφέρουμε

- ΄Υπαρξη δεύτερου τροφοδοτικού (Redundant Power Supply)
- ΄Υπαρξη RAID 5 στο Data και RDBMS Server με ύπαρξη hot spare δίσκου ο οποίος τίθεται σε λειτουργία αυτόματα και χτίζεται εκ νέου από τους υπόλοιπους δίσκους χωρίς φυσική παρέμβαση.
- ΄Υπαρξη RAID 1/0 (mirror) στους Domain Controllers έτσι ώστε να υπάρχει και εκεί παρόμοια δυνατότητα για ανοχή σε τυχόν αστοχία υλικού.
- Διπλές κάρτες δικτύου στα προαναφερθέντα μηχανήματα σε τυχόν αστοχία υλικού.
- Τήρηση αντιγράφου ασφαλείας σε επίπεδο μηχανημάτων (Data Server & Domain Controllers). Η διαδικασία είναι αυτοματοποιημένη και το backup έχει φορτωθεί με επιτυχία σε δοκιμαστικά μηχανήματα (VMs)

- Αυτοματοποιημένη διαδικασία λήψεως αντιγράφων ασφαλείας με χρονο-προγραμματισμένες εργασίες σε επίπεδο και σταθμών εργασίας αλλά και Server (Scheduled Backup Tasks και Chrontab)
- Για τους σταθμούς εργασίας λήψη αντιγράφου ασφαλείας και αποστολή αυτού στο σε τρίτο μηχάνημα (File Server)
- Για το RDBMS λήψη αντιγράφου ασφαλείας και τήρηση αυτού στο ίδιο το μηχάνημα και αποστολή αντιγράφου σε τρίτο μηχάνημα (File Server)
- Λήψη αντιγράφου ασφαλείας του File Server σε external storage device (Portable NAS-Network Attached Storage-) το οποίο φυλάσσεται σε διαφορετικό ασφαλές χώρο πέραν του Computer Room, από εξουσιοδοτημένο προσωπικό της εταιρίας.
- Ύπαρξη συστήματος αδιάλειπτης λειτουργίας UPS (με σταθεροποιητή τάσης) και στους εξυπηρετητές αλλά και σε σταθμούς εργασίας.

ΕΠΙΛΟΓΟΣ

Παρουσιάστηκε λοιπόν ένας ολοκληρωμένος κατάλογος των διαδικασιών προστασίας δεδομένων για την εταιρία της εργασίας μας, καθώς και η εφαρμογή τους για την υλοποίηση της πολιτικής ασφαλείας.

Κατά τη διάρκεια του development λαμβάνονται μέτρα ασφάλειας όπως προβλέπονται στα policies (Domain, Access Control, Disk encryption, Dummy Data etc). Από τη στιγμή που θα βγει το εκτελέσιμο και πριν γίνει το roll out στους πελάτες υπάρχει δοκιμαστική περίοδος σε επιλεγμένους χρήστες (Super Users) από τους οποίους γίνεται ένα αρχικό beta testing σε ασφαλές εκ των πραγμάτων περιβάλλον (Κλειστό δίκτυο ΣΥΖΕΥΞΙΣ).

ΣΥΜΠΕΡΑΣΜΑΤΑ

Σκοπός της παρούσας εργασίας είναι να περιγράψει τις βασικές αρχές που διέπουν το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Σ.Δ.Α.Π.) και Πληροφοριακών Συστημάτων μιας εταιρίας που δραστηριοποιείται στο χώρο της παραγωγής ολοκληρωμένων πληροφοριακών συστημάτων **.**

Παρέχει την ανάπτυξη για την εφαρμογή Πολιτικών, υποστηρικτικών Διεργασιών, Διαδικασιών και Συστημάτων ώστε να αποπνέει εμπιστοσύνη για την ασφαλή διαχείριση πληροφοριών σε κάθε συναλλασσόμενο με την εταιρεία.

Ειδικότερα, περιλαμβάνει προβλέψεις για:

- τον καθορισμό των Πολιτικών Ασφαλείας που πρέπει να τηρούνται για την ορθή χρήση των πληροφοριακών συστημάτων την εταιρεία,
- τον προσδιορισμό των χρηστών, των ρόλων και δικαιωμάτων πρόσβαση και χρήσης πληροφοριακών συστημάτων,
- μέτρα αντιμετώπισης παραβιάσεων ασφαλείας,
- μηχανισμούς για έκτακτη ανάκαμψη και λειτουργία στη περίπτωση απώλειας πληροφοριών και στοιχείων ή/και παραβίασης ασφάλειας.

Στόχος αποτελεί η εφαρμογή Σ.Δ.Α.Π. για την προστασία των Η/Υ, περιφερειακών συστημάτων, δικτύων και των αποθηκευμένων σε αυτά πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, χρήση, αλλοίωση ή καταστροφή (απώλεια).

Η παρούσα εργασία εκπονήθηκε σύμφωνα με τις απαιτήσεις του διεθνούς προτύπου ISO 27001:2013 και του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR).

Η εργασία αυτή απευθύνεται σε οποιονδήποτε εμπλέκεται στην εφαρμογή του Συστήματος Διαχείρισης Ασφάλεια Πληροφοριών της εταιρείας και ειδικότερα:

- στη Διοίκηση για τον καθορισμό πολιτικών, στόχων και δεικτών αποδοτικότητας και αποτελεσματικότητας,
- στον Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών, που έχει ως αποστολή την επίβλεψη της εφαρμογής και συνεχή βελτίωση ολόκληρου του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Σ.Δ.Α.Π.),
- στους Υπεύθυνους των επιμέρους Διεργασιών και των διαδικασιών που απαρτίζουν το Σύστημα, και έχουν την ευθύνη του αναλυτικού σχεδιασμού και της εφαρμογής του,

- σε όλο το προσωπικό της εταιρείας που εμπλέκεται στην εφαρμογή του, καθώς και
- στους συνεργάτες του,
- σε φορείς πιστοποίησης, πελάτες και εξωτερικούς ελεγκτές,
- σε οποιονδήποτε επηρεάζεται από τη δραστηριότητα της εταιρίας.

Τεχνική Ορολογία Συστήματος Ασφάλειας Πληροφοριών

- Πολιτική για την Ασφάλεια Πληροφοριών (Information security Policy): Το σύνολο των προθέσεων συναφών με την Ασφάλεια Πληροφοριών, όπως εκφράζονται επίσημα από την Ανώτατη Διοίκηση.
- Στόχοι (Security policy objectives): Στόχοι που τίθενται για την ασφαλεία πληροφοριών και τον καθορισμό περιορισμών.
- Σύστημα Διαχείρισης της Ασφάλειας Πληροφοριών (Information Security Management System): Σύστημα Διαχείρισης για τη Διοίκηση και τον έλεγχο της εταιρίας όσον αφορά την Ασφάλεια Πληροφοριών.
- Διεργασία: Σύνολο αλληλοσχετιζόμενων ή αλληλοεπιδράσεων δραστηριοτήτων το οποίο μετασχηματίζει εισερχόμενα σε εξερχόμενα.
- Διαδικασία: Καθορισμένος τρόπος για την εκτέλεση μιας δραστηριότητας ή μίας Διεργασίας
- Πελάτης/Συναλλασσόμενος: Οργανισμοί – Τράπεζες, Ιδιωτικός και δημόσιο τομέας.

Κατανόηση απαιτήσεων ενδιαφερομένων μερών

Ο οργανισμός έχει καθορίσει τα ενδιαφερόμενα μέρη από την λειτουργία του και έχει εντοπίσει τις ανάγκες τους στα πλαίσια της ασφάλειας πληροφοριών μέσω της διαδικασίας αξιολόγησης της επικινδυνότητας που εφαρμόζει.
Τα βασικά ενδιαφερόμενα μέρη του οργανισμού είναι:

- Οι τελικοί χρήστες – πελάτες των υπηρεσιών – λογισμικού
- Προμηθευτές – διανομείς και όλοι η αλυσίδα προμηθειών
- Οι κανονισμοί και η νομοθεσία που διέπει την ασφάλεια δεδομένων
- Η ωφελούμενοι από την χρήση των προϊόντων – υπηρεσιών που παρέχει.

Μέτρο της επιτυχίας του συστήματος, είναι η επίτευξη συγκεκριμένων στόχων και η εμφύσηση εμπιστοσύνης για την ακεραιότητα, και ασφάλεια πληροφοριών σε όλους του εμπλεκόμενους. Για τους λόγους αυτούς η εταιρία:

- Αναπτύσσει και εφαρμόζει Πολιτικές και Διαδικασίες, που εξειδικεύουν την Πολιτική και διασφαλίζουν την ακεραιότητα πληροφοριών από εσωτερικούς και εξωτερικούς κινδύνους
- Εμπνέει εμπιστοσύνη σε κάθε εμπλεκόμενο πως ενεργεί σύμφωνα με επικυρωμένα διεθνή πρότυπα, νόμους και κανονισμούς, καθώς και συμβατικές απαιτήσεις για την ασφάλεια πληροφοριακών συστημάτων
- Προστατεύει τα περιουσιακά της στοιχεία και πληροφορίες από απειλές εσωτερικές και εξωτερικές και κινδύνους.
- Διασφαλίζει την ασφαλή διατήρηση εμπιστευτικών πληροφοριών και διαφυλάττει τη μη εξουσιοδοτημένη πρόσβαση
- Βελτιώνει συνεχώς το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών με τη δημιουργία και την τακτική αναθεώρηση των μετρήσιμων στόχων ασφάλειας, των σχετικών λειτουργιών της οργάνωσης
- Εφαρμόζει διαδικασίες για τον εντοπισμό και αξιολόγηση κινδύνων και των επιπτώσεών τους σε προστατευόμενες πληροφορίες
- Προβαίνει σε όλες τις απαραίτητες ενέργειες, ώστε να επικοινωνήσει την πολιτική αλλά και τις εξειδικευμένες Πολιτικές Ασφαλείας σε κάθε εμπλεκόμενο.

ΑΝΑΦΟΡΕΣ

1. https://eur-lex.europa.eu/homepage.html?locale=el
2. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm
3. https://gdpr-info.eu/
4. http://www.elot.gr/
5. https://www.itsecuritypro.gr/gdpr-ypochreosis-symmorfosis-ston-geniko-kanonismo-prosopikon-dedomenon/

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική Βιβλιογραφία

Αλεξανδροπούλου – Αιγυπτιάδου, Ε. (2002), Ζητήματα από το Δίκαιο της Πληροφορικής. Αθήνα - Θεσσαλονίκη: Α. Σάκκουλας.

Αρκουλή, Κ.Γ. (2010), Προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες. Αθήνα: Νομική Βιβλιοθήκη.

Μήτρου, Λ. (2017), Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων. Αθήνα – Θεσσαλονίκη: Α. Σάκκουλας.

Ξενόγλωσση Βιβλιογραφία

Arnason S.T. & Willett K.D. (2007). How to Achieve 27001 Certification: An Example of Applied Compliance Management. Auerbach Publications, New York

Ashenden D. (2008). Information Security Management: A human challenge. Information Security Technical Report 13(4), 195-201.

ISO/IEC 27000:2005 Information technology – Security techniques – Information security management systems – Overview and vocabulary. Ελληνικός Οργανισμός Τυποποίησης (ΕΛΟΤ).

ITGP Privacy Team. EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second edition. IT Governance Publishing

Roland Costea (2018). Build EU GDPR Data Protection Compliance from Scratch (CIPT). Packt Publishing

ΠΑΡΑΡΤΗΜΑΤΑ

Στο παρακάτω σχήμα παρουσιάζεται το οργανόγραμμα της εταιρίας: