1. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ PALADINO

1.1. ΠΑΡΟΥΣΙΑΣΗ ΚΑΙ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας Πληροφοριών έχει σχεδιαστεί έτσι ώστε να παρουσιάζονται όλοι οι μηχανισμοί αναγνώρισης, αξιολόγησης, εφαρμογής και ελέγχου μηχανισμών ασφαλείας για όλες τις επιμέρους πτυχές της ασφάλειας πληροφοριών.

Η Πολιτική διαθέτει αρθρωτή δομή και γίνεται επιμέρους ανάλυση των θεμάτων που σχετίζονται με την ασφάλεια πληροφοριών.

Η παρούσα Πολιτική εφαρμόζεται σε όλες τις λειτουργίες και δραστηριότητες της εταιρείας και σε όλες τις δομές και υποδομές της.

1.2. ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΠΟΛΙΤΙΚΗΣ

Η Εταιρεία ΠΑΛΑΝΤΙΝΟ Α.Ε. παρέχει υπηρεσίες διαχείρισης πελατοκεντρικών σχέσεων και εμπορικών απαιτήσεων για λογαριασμό τρίτων επιχειρήσεων.

Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών σχεδιάστηκε και εφαρμόζεται με στόχο:

- Να αποτελέσει τον βασικό μηχανισμό για τη βέλτιστη οργάνωση και λειτουργία της Εταιρείας **προσδιορίζοντας παράλληλα το πλαίσιο λειτουργίας της**
- Να αναγνωρίσει τα **ενδιαφερόμενα μέρη** και τις απαιτήσεις τους καθώς είναι κρίσιμα για την ασφάλεια των πληροφοριών που διαχειρίζεται η Εταιρεία
- Να **διασφαλίσει** την ορθή διαχείριση των πληροφοριών που επεξεργάζεται η Εταιρεία
- Να **διασφαλίσει την επιχειρησιακή συνέχεια** των διεργασιών που κρίνονται κρίσιμες
- Να εντοπίσει και να **αξιοποιήσει ευκαιρίες** όπως επίσης να **αντιμετωπίσει απειλές** που συνδέονται με το επιχειρησιακό της περιβάλλον ενισχύοντας έτσι το επίπεδο ασφαλείας της εταιρείας
- Να **εξασφαλίσει έγκαιρη και αποτελεσματική** διαχείριση τυχόν περιστατικών ασφαλείας
- Να **εξασφαλίσει** το απαιτούμενο επίπεδο **κατανόησης** και **ευαισθητοποίησης** του προσωπικού της εταιρείας σε θέματα ασφάλειας πληροφοριών, δικτύων και υποδομών

Η Εταιρεία δεσμεύεται για τη συμμόρφωση με τις **απαιτήσεις** (νομικές και προδιαγραφές πελατών) που διέπουν τις υπηρεσίες της και την διαχείριση δεδομένων, και για τη συνεχή βελτίωση της αποτελεσματικότητας του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

Η Εταιρεία που εφαρμόζει το σύστημα και διατηρεί πιστοποιητικό σύμφωνα με το ISO 27001:2013, διαθέτει ειδικό Εγχειρίδιο στο οποίο περιγράφεται το πεδίο εφαρμογής του Συστήματος. Παράλληλα, η εταιρεία έχει τεκμηριώσει σε ειδικό έγγραφο όλες τις επιμέρους Πολιτικές Ασφαλείας που διέπουν την οργάνωση και λειτουργία της.

Η Διοίκηση της Εταιρείας, λαμβάνοντας συνεχώς υπόψη τις τεχνολογικές εξελίξεις και τις αλλαγές στο νομικό πλαίσιο που διέπει την προστασία των δεδομένων, θέτει μια σειρά στόχων που αφορούν στην βελτίωση της επίδοσης και του επιπέδου ασφαλείας. Οι στόχοι και η επίτευξή τους, καθώς και η θέσπιση νέων στόχων, εξετάζονται στα πλαίσια της ετήσιας ανασκόπησης του ενιαίου Συστήματος Διαχείρισης.

Η Διοίκηση της Εταιρείας επενδύει συστηματικά σε τεχνολογικές και λειτουργικές επεμβάσεις προκειμένου να μπορεί να εξασφαλίζει διαρκή βελτίωση του επιπέδου ασφαλείας.

Όλα τα εμπλεκόμενα μέρη της Εταιρείας υποχρεούνται να εφαρμόζουν το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.

Το περιεχόμενο της Πολιτικής Ασφάλειας Πληροφοριών εξετάζεται ετησίως ως προς την καταλληλότητά του κατά την ανασκόπηση από τη Διοίκηση.

Η Πολιτική Ασφάλειας Πληροφοριών της Εταιρείας είναι στη διάθεση κάθε ενδιαφερομένου.

1.3. ΑΝΑΛΥΣΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Παρακάτω αναλύονται όλες οι επιμέρους ενότητες της Πολιτικής Ασφάλειας Πληροφοριών της Εταιρείας.

1.3.1. ΟΡΓΑΝΩΤΙΚΗ ΔΟΜΗ – ORGANIZATIONAL STRUCTURE

Η Εταιρεία διαθέτει προκαθορισμένη οργανωτική δομή, η οποία αξιοποιείται τόσο στις επιμέρους Πολιτικές (πχ Πολιτική Ελέγχου Πρόσβασης) όσο και στην τεκμηρίωση του Ενιαίου Συστήματος Διαχείρισης το οποίο εφαρμόζει η εταιρεία. Υπάρχει πλήρης αντιστοίχιση των ρόλων και των στοιχείων των κατόχων αυτών, ενώ προβλέπονται διεργασίες στο σύστημα διαχείρισης για την ενσωμάτωση των αλλαγών που γίνονται τόσο σε επίπεδο φυσικών προσώπων όσο και σε επίπεδο οργανογράμματος.

Το οργανόγραμμα της εταιρείας παρουσιάζεται στο Εγχειρίδιο του Ενιαίου Συστήματος Διαχείρισης της Εταιρείας.

1.3.2. ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ – RISK MANAGEMENT

Όλος ο στρατηγικός σχεδιασμός της εταιρείας βασίζεται στην αποτύπωση και ανάλυση των πηγών κινδύνων που σχετίζονται με την ασφάλεια πληροφοριών. Σε ετήσια βάση γίνεται η επαναξιολόγηση των δεδομένων στα οποία βασίζεται η ανάλυση και αξιολόγηση των κινδύνων, και σε περίπτωση μεταβολών επικαιροποιείται το σύνολο της ανάλυσης κινδύνων. Παράλληλα, αλλαγές στην εταιρεία δύναται να οδηγήσουν στην ανάγκη επικαιροποίησης της ανάλυσης κινδύνων.

Η μεθοδολογία ανάλυσης και αξιολόγησης κινδύνων βασίζεται στην καταγραφή και ανάλυση του πλαισίου λειτουργίας, των αναγκών και προσδοκιών των ενδιαφερόμενων μερών, των δυνατών και αδύναμων σημείων σχετικά με τις εσωτερικές παραμέτρους που επηρεάζουν την λειτουργία της εταιρείας και αντίστοιχα των απειλών και ευκαιριών που σχετίζονται με τις εξωτερικές παραμέτρους λειτουργίας.

1.3.3. ΔΙΑΧΕΙΡΙΣΗ ΦΟΡΗΤΩΝ ΜΕΣΩΝ – MOBILE DEVICES

Η Εταιρεία, για την αποτελεσματικότερη προστασία της ασφάλειας των πληροφοριών, δεν επιτρέπει τη χρήση μεταφερόμενων μέσων κατά κανόνα. Για το λόγο αυτό έχουν εφαρμοστεί και ειδικά μέτρα προστασίας που δεν επιτρέπουν την χρήση εξωτερικών δίσκων και usb στα τερματικά των χρηστών.

Καθορισμένοι ρόλοι, διοικητικού επιπέδου, δύναται να απαιτηθεί να κάνουν χρήση μεταφερόμενων μέσων για την εκτέλεση των εργασιών τους. Η έγκριση χρήσης τέτοιων μέσων γίνεται μέσω της Διαχείρισης προσβάσεων της παρούσας πολιτικής.

Για τις περιπτώσεις όπου γίνεται χρήση των μεταφερόμενων μέσων, κατά περίπτωση και ανά είδος μέσου, ο IS Manager έχει τεκμηριώσει επιπλέον μηχανισμούς ασφαλείας που εφαρμόζονται στα μέσα αυτά.

Τέλος, η εταιρεία διατηρεί διεργασίες για την ασφαλή καταστροφή των φορητών μέσων. Οι διεργασίες αυτές προβλέπουν ειδικές μεθόδους καταστροφής για την διασφάλιση της οριστικής διαγραφής δεδομένων καθώς και τεκμηρίωση των ενεργειών καταστροφής σε σχετικά αρχεία.

1.3.4. ΑΝΘΡΩΠΙΝΟΙ ΠΟΡΟΙ – HUMAN RESOURCES

Η εταιρεία διαθέτει διεργασίες για την επιλογή (screening) του προσωπικού καθώς και για την ορθή ένταξη νέων εργαζομένων στην εργασία τους, πάντα με γνώμονα την τήρηση των Πολιτικών και Κανονισμών Λειτουργίας της εταιρείας. Για το λόγο αυτό η εταιρεία υλοποιεί τα παρακάτω:

1. Screening με κριτήρια που συμβαδίζουν και με τις απαιτήσεις πελατών για την διασφάλιση της καταλληλότητας, επάρκειας και ακεραιότητας του προσωπικού
2. Γνωστοποίηση και λήψη δέσμευσης συμμόρφωσης με Πολιτικές και Κανονισμούς Λειτουργίας εταιρείας (τα εν λόγω έγγραφα κάνουν σαφή αναφορά ενδεικτικά σε ασφάλεια πληροφοριών και προστασία δεδομένων, διαχείριση παγίων, εχεμύθεια και εμπιστευτικότητα, πρόληψη δωροδοκίας, και άλλα)
3. Induction training σε όλους τους εργαζόμενους (διοικητικό προσωπικό και agents) αμέσως μετά την πρόσληψή τους – η θεματολογία του induction training καλύπτει τα εξής πεδία: job related training, Οργάνωση και Λειτουργία εταιρείας, Εκπαίδευση στο Ενιαίο Σύστημα Διαχείρισης, Υγεία και Ασφάλεια στον χώρο εργασίας, Ασφάλεια Πληροφοριών, Διαχείριση Προσωπικών Δεδομένων
4. Awareness Assessment για την διαρκή αξιολόγηση του επιπέδου ευαισθητοποίησης και κατανόησης του προσωπικού σε θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων
5. Αξιολόγηση προσωπικού σε συνεχή βάση με στόχο τη διαρκή βελτίωση και την πρόληψη λαθών κατά την επεξεργασία δεδομένων της εταιρείας
6. Low Performer Assessment προκειμένου να διασφαλίζεται ότι εργαζόμενοι με χαμηλές αποδόσεις αναγνωρίζονται και βελτιώνονται. Αν αυτό δεν είναι εφικτό τότε υλοποιούνται ενέργειες λύσης συνεργασίας.

1.3.5. ΔΙΑΧΕΙΡΙΣΗ ΠΑΓΙΩΝ – ASSET MANAGEMENT

Η εταιρεία αναγνωρίζει, καταγράφει και εφαρμόζει κανόνες για την ορθή διαχείριση και προστασία αυτών. Υπάρχει πλήρης καταγραφή των παγίων, απόδοση αναγνωριστικών αυτών, καταγραφή της θέσης του κάθε παγίου, αναγνώριση του owner του παγίου και καταγραφή του ιστορικού των αλλαγών σε αυτό. Παράλληλα, η εταιρεία διαθέτει διεργασίες για την χρέωση και αποχρέωση εξοπλισμού πάντα σε συμμόρφωση με το προφίλ κάθε ρόλου και τους πόρους που προβλέπεται να έχει.

Για κάθε τερματικό υπάρχει προτυποποιημένο προφίλ με βάση τη θέση εργασίας.

Όλες οι αλλαγές σε πάγια ακολουθούν μια διεργασία εγκρίσεων, ενώ πάντα τεκμηριώνονται και σχεδιάζονται οι αλλαγές αυτών και οι προδιαγραφές ασφαλείας που θα τηρηθούν.

1.3.6. ΔΙΑΒΑΘΜΙΣΗ ΠΛΗΡΟΦΟΡΙΩΝ – INFORMATION CLASSIFICATION

Η εταιρεία έχει σχεδιάσει σύστημα διαβάθμισης πληροφοριών βάση του οποίου έχουν καθοριστεί και οι αποδεκτές μέθοδοι διαχείρισης των πληροφοριών με βάση την διαβάθμιση των δεδομένων.

1.3.7. ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΕΩΝ – ACCESS CONTROL

Η εταιρεία έχει σχεδιάσει διεργασίες για τον έλεγχο των προσβάσεων. Ο σχεδιασμός βασίζεται στην δημιουργία προφίλ χρηστών με βάση τον ρόλο του κάθε χρήστη και την οργανική οντότητα στην οποία ανήκει ο κάθε χρήστης.

Η απόδοση πρόσβασης γίνεται κατόπιν σχετικών αιτημάτων και αντίστοιχων εγκρίσεων αυτών. Έχουν καθοριστεί οι ρόλοι που έχουν το δικαίωμα έγκρισης και άρσης όλων των δικαιωμάτων πρόσβασης και ειδικότερα privileged δικαιώματα. Η εταιρεία εφαρμόζει διεργασίες για την ορθή διαχείριση των κωδικών πρόσβασης στα συστήματα.

Παράλληλα, με την διαρκή συνεργασία των διευθύνσεων της εταιρείας, διασφαλίζεται ότι οι εταιρείες διαθέτουν διαρκή έλεγχο τόσο στην απόδοση όσο και στην άρση των δικαιωμάτων αλλά και σε περιπτώσεις μεταβολών αυτών.

Για την διασφάλιση της προστατευόμενης πρόσβασης σε συστήματα και εφαρμογές, η εταιρεία έχει θέσει σε λειτουργία μηχανισμούς ελέγχου πρόσβασης σε επίπεδο δικτύου και εφαρμογών και κάθε χρήστης λαμβάνει μοναδικούς συνδυασμούς ονομάτων χρηστών και κωδικών πρόσβασης για κάθε σύστημα και εφαρμογή. Η πολιτική που τηρείται για τόσο για τα ονόματα πρόσβασης, όσο και για τους κωδικούς (συχνή αλλαγή, υψηλό επίπεδο πολυπλοκότητας, χρήση ιστορικού κωδικών, κτλ) διασφαλίζει υψηλό επίπεδο ασφαλείας για την πρόσβαση στα συστήματα και τις εφαρμογές.

Ειδικά μέτρα λαμβάνονται για την απόδοση και έλεγχο πρόσβασης σε χρήστες υψηλής διαβάθμισης (privileged users) καθώς και σε χρήστες που λαμβάνουν δικαίωμα απομακρυσμένης πρόσβασης (remote access rights). Και στις δύο περιπτώσεις αυτές η εταιρεία έχει υιοθετήσει μηχανισμό ελέγχου πρόσβασης πολλαπλών παραγόντων (2FA).

Η εταιρεία εκτελεί συστηματικούς ελέγχους των δικαιωμάτων πρόσβασης (review) προκειμένου να διασφαλίζει την απόδοση της διεργασίας απόδοσης και ελέγχου πρόσβασης.

1.3.8. ΚΡΥΠΤΟΓΡΑΦΗΣΗ – CRYPTOGRAPHY

Η εταιρεία κάνει χρήση κρυπτογράφησης με στόχο την αύξηση της προστασίας των δεδομένων, όταν αυτά βρίσκονται αποθηκευμένα σε βάσεις δεδομένων (TDE encryption for databases) και σε αντίγραφα ασφαλείας. Επιπλέον εφαρμογές που χρησιμοποιεί η εταιρεία για απομακρυσμένη πρόσβαση διασφαλίζουν την κρυπτογράφηση των καναλιών επικοινωνίας. Σε φορητούς σταθμούς εργασίας εφαρμόζεται οριζόντια μέτρο κρυπτογράφησης (laptop encryption) με την χρήση εφαρμογής bitlocker.

Στο Σύστημα Διαχείρισης προβλέπεται η καταγραφή και διαχείριση μηχανισμών ασφαλείας που σχετίζονται με την κρυπτογράφηση των δεδομένων.

1.3.9. ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ – PHYSICAL SECURITY

Η εταιρεία έχει δημιουργήσει και εφαρμόζει διεργασίες για τον σχεδιασμό και την τήρηση προδιαγραφών ασφαλείας κατά την φυσική πρόσβασης στις εγκαταστάσεις. Οι χώροι της εταιρείας έχουν ειδική διαβάθμιση ως προς την επιτρεπόμενη πρόσβαση σε αυτούς. Η πρόσβαση ελέγχεται μέσω συστήματος καρτών φυσικής πρόσβασης. Σε ειδικές περιπτώσεις υπάρχει και επιπλέον σημείο ελέγχου πρόσβασης με τη χρήση κωδικών για την είσοδο (πχ Back Office, Computer Room).

Οι κάρτες πρόσβασης είναι μοναδικές για κάθε χρήστη και σχετίζονται τα δικαιώματα αυτής με τον γενικό σχεδιασμό των κανόνων απόδοσης δικαιωμάτων πρόσβασης της εταιρείας.

Η εταιρεία διαθέτει κεντρική είσοδο με ελεγχόμενη πρόσβαση, ενώ παράλληλα τηρείται διεργασία για την διαχείριση των επισκεπτών της εταιρείας (η οποία γίνεται με συνοδεία) και την διαχείριση τρίτων μερών (συνεργατών και πελατών) που αποκτούν δικαιώματα πρόσβασης.

Η διεργασία απόδοσης δικαιωμάτων πρόσβασης ελέγχεται συστηματικά για την διασφάλιση της τήρησης των προδιαγραφών της εταιρείας.

1.3.10. ΑΣΦΑΛΕΙΑ ΠΕΡΙΒΑΛΛΟΝΤΟΣ – ENVIRONMENTAL PROTECTION

Ο εξοπλισμός της εταιρείας είναι τοποθετημένος με τέτοιο τρόπο ώστε να προστατεύεται στο μέγιστο βαθμό από περιβαλλοντικές συνθήκες που δύναται να επηρεάσουν την κατάστασή του. Ο σχεδιασμός της τοποθέτησης του εξοπλισμού υλοποιείται με βάση διεργασίες διαχείρισης παγίων.

Η εταιρεία διαθέτει πλήρως εξοπλισμένο Computer Room με συστήματα παρακολούθησης περιβαλλοντικών συνθηκών για την διασφάλιση της προστασίας των κεντρικών παραγωγικών μονάδων. Τόσο στον χώρο αυτό όσο και στο σύνολο της εταιρείας, έχει εγκατασταθεί και συντηρείται ένα πλήρως αποτυπωμένο δίκτυο, ενώ για την συνέχιση της λειτουργίας της εταιρείας, οι υποδομές υποστηρίζονται τόσο από ups όσο και από γεννήτρια.

Επίσης, υπάρχουν προκαθορισμένοι χώροι για την παραλαβή και παράδοση αγαθών, με ελεγχόμενη πρόσβαση, και διαχωρισμό φυσικής πρόσβασης σε σχέση με λοιπές μονάδες της εταιρείας.

1.3.11. ΛΕΙΤΟΥΡΓΙΕΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΑΛΛΑΓΩΝ – OPERATIONS AND CHANGE MANAGEMENT

Η εταιρεία διαθέτει τεκμηριωμένες διαδικασίες για την ακριβή αποτύπωση των λειτουργιών όλων των τμημάτων που σχετίζονται με τις υποδομές και τα συστήματα καθώς και των Διευθύνσεων που σχετίζονται με την Ασφάλεια Πληροφοριών και τα Προσωπικά Δεδομένα. Οι διεργασίες αυτές περιλαμβάνουν μεταξύ άλλων την ελεγχόμενη υλοποίηση καθημερινών εργασιών του ICT, την παρακολούθηση του capacity των παραγωγικών και υποστηρικτικών συστημάτων και υποδομών, τον έλεγχο καλής εκτέλεσης των αυτοματοποιημένων εργασιών και μηχανισμών ασφαλείας.

Παράλληλα, υπάρχουν διεργασίες διαχείρισης αλλαγών μέσα από τις οποίες γίνεται η καταγραφή και αξιολόγηση όλων των παραμέτρων που δύναται να επηρεάσουν την εταιρεία σε θέματα ασφάλειας, ακεραιότητας και διαθεσιμότητας συστημάτων και πληροφοριών.

1.3.12. ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΙΟΥΣ – MALWARE PROTECTION

Το σύνολο των υποδομών και συστημάτων προστατεύονται με κατάλληλες εφαρμογές από ιούς. Υπάρχουν συστηματικές διεργασίες για τον έλεγχο και εγκατάσταση των updates των εφαρμογών αυτών τόσο σε κεντρικά συστήματα όσο και σε τερματικούς σταθμούς.

1.3.13. ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ – BACK UP

Η εταιρεία έχει δημιουργήσει διεργασίες για την κατάλληλη επιλογή και τον σχεδιασμό του backup με στόχο να λαμβάνονται όλες οι υποδομές σε αντίγραφα ασφαλείας, με κριτήριο το είδος των δεδομένων που περιέχουν. Η συχνότητα λήψης των αντιγράφων ασφαλείας ποικίλει ανά σύστημα και υποδομή. Το σύνολο της αρχιτεκτονικής αυτής είναι τεκμηριωμένο σε αντίστοιχα αρχεία.

Διενεργούνται συστηματικοί έλεγχοι προκειμένου να διασφαλιστεί ότι τα αντίγραφα ασφαλείας είναι διαθέσιμα και τα δεδομένα είναι πλήρη και δεν έχουν αλλοιωθεί.

1.3.14. ΚΑΤΑΓΡΑΦΗ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΕΝΕΡΓΕΙΩΝ – LOGGING AND MONITORING

Η εταιρεία διατηρεί μεθόδους συλλογής και αξιολόγησης αρχείων καταγραφής των υποδομών της. Οι μέθοδοι συλλογής και αξιολόγησης αυτών ποικίλουν και σχετίζονται με τις εκάστοτε εφαρμογές και τα συστήματα των οποίων τα αρχεία συλλέγονται. Η εταιρεία έχει επιλέξει λοιπόν τα αρχεία καταγραφών που κατά περίπτωση είναι κρίσιμα και ουσιαστικά για την παρακολούθηση ενεργειών στα συστήματα και τις εφαρμογές.

Η εταιρεία διαθέτει μηχανισμούς alerting με βάση τα αρχεία καταγραφής (log files) προκειμένου να διασφαλίζεται ότι τυχόν περιστατικά μη εξουσιοδοτημένης πρόσβασης ή κακόβουλης χρήσης προλαμβάνονται εγκαίρως.

Η εταιρεία, με βάση και τα αποτελέσματα του risk assessment που διενεργεί τακτικά, έχει καθορίσει ανά κρίσιμο πόρο τις αναγκαίες καταγραφές ενεργειών (log files). Οι πόροι αυτοί ενδεικτικά είναι: Domain Controllers, Database Servers, File Servers, Firewalls.

1.3.15. ΔΙΑΧΕΙΡΙΣΗ ΤΡΩΤΟΤΗΤΩΝ – VULNERABILITY MANAGEMENT

Η εταιρεία αναγνωρίζει τις τρωτότητες των Συστημάτων της που οδηγούν σε αδυναμίες ασφάλειας μέσω του ελέγχου των δικτύων, των συστημάτων και των εφαρμογών της για γνωστές τρωτότητες καθώς και μέσα από σχετική ενημέρωση των διαφόρων προμηθευτών συστημάτων.

Οι έλεγχοι πραγματοποιούνται ανάλογα με την επικινδυνότητα των συστημάτων και την σημαντικότητα των πληροφοριών που διαχειρίζονται. Οι έλεγχοι γίνονται συστηματικά από το Τμήμα ICT σε συγκεκριμένο προγραμματισμό ή και σε έκτακτες περιπτώσεις αλλά και από εξωτερικούς εξειδικευμένους συνεργάτες.

Όλες οι τρωτότητες που αναγνωρίζονται, αξιολογούνται για την κρισιμότητά τους και προσδιορίζονται οι τρόποι αντιμετώπισης. Η Διοίκηση αξιολογεί τα δεδομένα, προσδιορίζει την προτεραιοποίηση των ενεργειών αντιμετώπισης και εγκρίνει τα σχετικά σχέδια.

1.3.16. ΔΙΚΤΥΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ – NETWORKS AND COMMUNICATIONS SECURITY

Η εταιρεία διαχειρίζεται την ασφάλεια των Δικτύων και των Επικοινωνιών μέσα από διάφορους εγκατεστημένους μηχανισμούς ασφαλείας, ενώ έχει παράλληλα υιοθετήσει πρακτικές για την ενσωμάτωση βάσει προδιαγραφών κατασκευαστών των βέλτιστων τεχνικών και πρακτικών ενίσχυσης ασφάλειας (system hardening).

Η επικοινωνία με το εξωτερικό περιβάλλον ελέγχεται μέσα από εγκατεστημένα και παραμετροποιημένα firewall ενώ γίνεται παρακολούθηση της κίνησης (traffic control) και των πρωτοκόλλων επικοινωνίας (protocol control).

Στο εσωτερικό περιβάλλον της εταιρείας υπάρχει διαχωρισμός Δικτύων καθώς και απομονωμένο Guest network. Η πρόσβαση στα δίκτυα ελέγχεται μέσω συγκεκριμένης password policy και Access Control Policy.

Η εταιρεία κάνει χρήση Microsoft 365 για την λειτουργικότητα της ηλεκτρονικής αλληλογραφίας των εργαζομένων της εταιρείας.

Η πρόσβαση στο διαδίκτυο είναι ελεγχόμενη για όλους τους χρήστες και το επίπεδο πρόσβασης δίδεται ανάλογα με τα δικαιώματα της συγκεκριμένης θέσης εργασίας.

1.3.17. ΠΡΟΜΗΘΕΙΑ, ΑΝΑΠΤΥΞΗ ΚΑΙ ΣΥΝΤΗΡΗΣΗ ΕΦΑΡΜΟΓΩΝ – SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Η εταιρεία έχει σχεδιάσει διεργασίες προκειμένου να λαμβάνονται κριτήρια που σχετίζονται με την ασφάλεια πληροφοριών κατά την προμήθεια, ανάπτυξη και συντήρηση εφαρμογών. Η εταιρεία εφαρμόζει διεργασίες για την ορθή επιλογή, αξιολόγηση και παρακολούθηση των προμηθευτών της. Παράλληλα κάθε αλλαγή στις υποδομές ως έργο αρχικώς αξιολογείται στα πλαίσια της διεργασίας Διαχείρισης Αλλαγών, οπότε και καθορίζονται όλα τα security requirements του έργου, τα οποία οφείλουν να ενσωματωθούν στην προμήθεια, ανάπτυξη ή συντήρηση εφαρμογών.

Εσωτερικές εργασίες ανάπτυξης και συντήρησης τεκμηριώνονται και παρακολουθούνται από την εταιρεία μέσα από ειδική εφαρμογή ticketing που χρησιμοποιεί. Σε κάθε περίπτωση οι αλλαγές στις υποδομές αρχικώς δοκιμάζονται σε testing environments και κατόπιν ελεγχόμενα τίθενται σε λειτουργία στις πραγματικές υποδομές της εταιρείας.

1.3.18. ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΜΗΘΕΙΩΝ – SUPPLIERS MANAGEMENT

Όλες οι προμήθειες που δύναται να επηρεάσουν την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών της εταιρεία είναι κρίσιμες προμήθειες και διέπονται από ειδική διεργασία βάση της οποίας γίνεται η επιλογή των προμηθευτών. Παράλληλα, οι διεργασίες προμηθειών προβλέπουν την διαρκή παρακολούθηση των προμηθευτών από supplies owners που ορίζονται από το αρχικό αίτημα προμήθειας.

Τέλος, σε ετήσια βάση γίνεται η επαναξιολόγηση όλων των προμηθευτών και αποτυπώνονται τα αποτελέσματα αυτών προς παρουσίαση στη Διοίκηση. Η εταιρεία κατά την Ανασκόπηση, αλλά και εκτάκτως, δύναται να εξαιρέσει προμηθευτές από τη λίστα εγκεκριμένων προμηθευτών.

1.3.19. ΔΙΑΧΕΙΡΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ – SECURITY INCIDENT MANAGEMENT

Η εταιρεία διατηρεί και εφαρμόζει διεργασία για την αναγνώριση και διαχείριση περιστατικών ασφαλείας. Μέσα στις διεργασίες αυτές προβλέπονται και πλάνα επικοινωνίας με τρίτα μέρη, εφόσον αυτά εμπλέκονται στην διαχείριση των περιστατικών ή επηρεάζονται από αυτά.

Προβλέπεται η τήρηση σε αρχείο όλων των περιστατικών ασφαλείας και της μεθόδου διαχείρισης αυτών. Ο τρόπος αναγγελίας τυχόν περιστατικού βασίζεται στην χρήση εφαρμογής ticketing, έτσι ώστε να διασφαλίζεται η άμεση και έγκαιρη ενημέρωση των υπευθύνων.

Οι διεργασίες που εφαρμόζονται για την διαχείριση περιστατικών ασφαλείας περιλαμβάνουν:

- αναλυτική περιγραφή των ρόλων και αρμοδιοτήτων,
- ενέργειες καταγραφής των περιστατικών,
- στάδια αξιολόγησης των περιστατικών για την ορθή λήψη αποφάσεων αναφορικά με την αντιμετώπισή τους,
- αξιοποίηση των αποτελεσμάτων από την διαχείριση των περιστατικών για την βελτίωση των μεθόδων και σχεδίων της εταιρείας και τελικώς
- συλλογή αποδεικτικών για την δημιουργία κατάλληλων αρχείων για την τεκμηρίωση των περιστατικών.

1.3.20. ΔΙΑΧΕΙΡΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΠΑΡΑΒΙΑΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ – DATA PRIVACY INCIDENTS

Ειδικά για τα περιστατικά παραβίασης προσωπικών δεδομένων, υπάρχει ειδική διεργασία που προβλέπει επιπλέον την επικοινωνία με αρμόδιες αρχές καθώς και τον Υπεύθυνο Επεξεργασίας, σε περίπτωση που η εταιρεία έχει το ρόλο του Εκτελούντος την Επεξεργασία. Η διεργασία αξιολόγησης του περιστατικού είναι διαφορετική καθώς έχει ως στόχο την αξιολόγηση της επίπτωσης στο υποκείμενο των δεδομένων από το περιστατικό.

1.3.21. ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ – BUSINESS CONTINUITY MANAGEMENT

Η εταιρεία έχει αναπτύξει και εφαρμόζει Διεργασίες Επιχειρησιακής Συνέχειας σύμφωνα με τις απαιτήσεις του ISO 22301. Οι Διεργασίες αυτές είναι εγκεκριμένες από την Διοίκηση και εφαρμόζονται σε όλο τον Οργανισμό. Από την εφαρμογή τους παράγονται αρχεία τα οποία διατηρούνται.

Η εταιρεία, στα πλαίσια εφαρμογής των απαιτήσεων του Προτύπου, εκτελεί Αξιολόγηση Κινδύνων (Risk Assessment) και Ανάλυση Επιχειρησιακών Επιπτώσεων (Business Impact Assessment). Κατά την Ανάλυση των Επιχειρησιακών Επιπτώσεων, τίθενται συγκεκριμένοι στόχοι Ανάκαμψης για όλες τις Κρίσιμες Διεργασίες.

Με βάση τα αποτελέσματα των αξιολογήσεων, καθορίζεται η στρατηγική ανάκαμψης της εταιρείας, με στόχο την πλήρη ή μερική επίτευξη των στόχων που έχουν τεθεί κατά την αξιολόγηση των Διεργασιών της εταιρείας. Οι προτεραιότητες που θέτει η εταιρεία για την αντιμετώπιση περιστατικού διαταραχής είναι οι εξής:

- Η Ασφάλεια του Προσωπικού, των Πελατών και του ευρύτερου κοινού

- Η προστασία των περιουσιακών στοιχείων και η τήρηση των υποχρεώσεων που έχει αναλάβει και διαχειρίζεται η εταιρεία
- Η συνέχιση πραγματοποίησης των εκτελούμενων από την εταιρία εργασιών και εξυπηρέτησης των πελατών

Για κάθε σενάριο κινδύνου, συντάσσεται λεπτομερές Σχέδιο Επιχειρησιακής Συνέχειας (BCP). Για κάθε σχέδιο προσδιορίζεται σαφώς:

- Ο στόχος του σχεδίου και το πεδίο εφαρμογής του
- Οι εμπλεκόμενες μονάδες της Εταιρείας
- Ο υπεύθυνος σύνταξης, ανασκόπησης και αναθεώρησης και οι υπεύθυνοι έγκρισης
- Οι συσχετίσεις του με άλλα Σχέδια καθώς και εξωτερικές προς την Εταιρεία απαιτήσεις συνέχειας
- Η διαδικασία ανάκαμψης Κρίσιμων Διεργασιών
- Η Διαδικασία επαναφοράς σε κανονική λειτουργία

Τα Σχέδια Επιχειρησιακής Συνέχειας τίθενται σε δοκιμαστική εφαρμογή, προκειμένου να επαληθευθεί η δυνατότητα υλοποίησής τους και η αποτελεσματικότητά τους ώστε να διασφαλιστεί ότι θα μπορέσουν να οδηγήσουν σε έγκαιρη ανάκαμψη σε περίπτωση πραγματικού περιστατικού.

1.3.22. ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΑΠΑΙΤΗΣΕΙΣ – COMPLIANCE

Η εταιρεία εφαρμόζει διεργασίες για την αναγνώριση και συμμόρφωση με νομοθετικές, κανονιστικές και συμβατικές απαιτήσεις.

Ειδικά αναφορικά με την συμμόρφωσης με τον Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR) η εταιρεία έχει ορίσει DPO και εφαρμόζει διεργασίες για την αναγνώριση και προστασία όλων των προσωπικών δεδομένων που διαχειρίζεται είτε ως Εκτελών είτε ως Υπεύθυνος Επεξεργασίας.

1.3.23. ΕΛΕΓΧΟΙ ΚΑΙ ΑΝΑΘΕΩΡΗΣΕΙΣ – REVIEWS

Η Πολιτική της Εταιρείας καθώς και όλο το σύστημα διαχείρισης ελέγχονται στα πλαίσια εσωτερικής επιθεώρησης καθώς και συστηματικών μηνιαίων ελέγχων εφαρμογής. Παράλληλα, σε ετήσια βάση γίνεται η ανασκόπηση των εγγράφων και οδηγιών της εταιρείας.

Επίσης, σε ετήσια βάση γίνεται αξιολόγηση της συμμόρφωσης της εταιρείας με τις απαιτήσεις του προτύπου ISO 9001 & ISO 27001 για τα οποία διατηρεί πιστοποιητικά συμμόρφωσης.

1.3.24. ΔΙΑΚΡΑΤΗΣΗ ΑΡΧΕΙΩΝ – RETENTION POLICY

Για όλα τα αρχεία, έχει καθοριστεί ο χρόνος διακράτησης καθώς και οι αρμοδιότητες για την διαγραφή αυτών. Για τον καθορισμό του χρόνου διακράτησης έχει ληφθεί υπόψη το είδος των δεδομένων (προσωπικά δεδομένα, επιχειρησιακά δεδομένα, κτλ) καθώς και νομοθετικές, κανονιστικές και συμβατικές υποχρεώσεις της εταιρείας που θέτουν προδιαγραφές αναφορικά με την διακράτηση.

Σε συνεχή βάση παρακολουθούνται οι χρόνοι διακράτησης και εφαρμόζονται διαγραφές αρχείων για όλες τις περιπτώσεις μη αυτοματοποιημένης διαγραφής.

1.4. ΠΙΝΑΚΑΣ ΠΕΔΙΩΝ ΠΟΛΙΤΙΚΗΣ