ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

ΟΡΓΑΝΩΤΙΚΑ ΚΑΙ ΤΕΧΝΙΚΑ ΜΕΤΡΑ

Η Ασφάλεια των Πληροφοριών επιτυγχάνεται όταν εφαρμόζονται και λειτουργούν απρόσκοπτα οι τρεις παρακάτω αρχές:

- Εμπιστευτικότητα – Confidentiality
- Ακεραιότητα – Integrity
- Διαθεσιμότητα – Availability

Παραβίαση προσωπικών δεδομένων συντελείται όταν παραβιαστεί μία από αυτές τις αρχές:

Παραβίαση Εμπιστευτικότητας: Οι πληροφορίες αποκαλύπτονται παρανόμως ή από αμέλεια σε μη εξουσιοδοτημένα πρόσωπα τα οποία αποκτούν πρόσβαση σε αυτές.

Παραβίαση Ακεραιότητας: Οι πληροφορίες αλλοιώνονται από παράνομη πράξη ή αμέλεια με αποτέλεσμα να καταστούν μη αξιόπιστες για την λειτουργία της επιχείρησης.

Παραβίαση διαθεσιμότητας: Οι πληροφορίες καθίστανται μη διαθέσιμες από παράνομη πράξη ή αμέλεια με αποτέλεσμα την αδυναμία λειτουργίας όλης της επιχείρησης ή τμημάτων της.

Α. Οργανωτικά Μέτρα Ασφαλείας

1. Διαχείριση Ασφαλείας Πληροφοριών

- Η ΓΕΩΡΓΙΑ ΜΑΡΑΓΚΟΥΔΑΚΗ (Υπεύθυνος Επεξεργασίας) έχει καθορίσει διακριτά την πολιτική που αφορά στην ασφαλή επεξεργασία των προσωπικών δεδομένων ως μέρος της Πολιτικής Ασφαλείας Πληροφοριών. Η εν λόγω πολιτική είναι εγκεκριμένη από την Διοίκηση και έχει κοινοποιηθεί σε όλους τους υπαλλήλους και όπου απαιτείται σε εξωτερικούς συνεργάτες. Η αναθεώρηση της πολιτικής διενεργείται, εφόσον απαιτείται, τουλάχιστον σε ετήσια βάση
- Η πολιτική ασφαλείας κατ' ελάχιστον αναφέρει:
    - τους ρόλους και τις υποχρεώσεις του προσωπικού
    - τα βασικά τεχνικά και οργανωτικά μέτρα που έχουν υιοθετηθεί για την ασφάλεια των προσωπικών δεδομένων, τους εκτελούντες την επεξεργασία ή τα τρίτα μέρη που συμμετέχουν στην επεξεργασία των προσωπικών δεδομένων.
- Ο Υπεύθυνος Επεξεργασίας τηρεί αρχείο με τις συγκεκριμένες πολιτικές και διαδικασίες που αφορούν στην ασφάλεια των προσωπικών δεδομένων.

2. Ρόλοι και Αρμοδιότητες

- Οι ρόλοι και οι αρμοδιότητες που αφορούν στην επεξεργασία των προσωπικών δεδομένων είναι σαφώς ορισμένοι σύμφωνα με την πολιτική ασφαλείας.
- Κατά την διάρκεια εσωτερικής αναδιοργάνωσης ή τερματισμού και τροποποίησης εργασιών, διενεργείται η ανάκληση των δικαιωμάτων και των αρμοδιοτήτων σύμφωνα με καταγεγραμμένες διαδικασίες.
- Έχουν οριστεί σαφώς οι αρμόδιοι για συγκεκριμένα καθήκοντα ασφαλείας πληροφοριών, συμπεριλαμβανομένου του ορισμού του υπευθύνου ασφαλείας πληροφοριών
- Ο υπεύθυνος ασφαλείας πληροφοριών έχει οριστεί από την Διοίκηση. Τα καθήκοντα και οι αρμοδιότητες του υπευθύνου ασφαλείας πληροφοριών είναι σαφώς καθορισμένα και καταγεγραμμένα
- Υφίσταται διαχωρισμός καθηκόντων και σχετικών αρμοδιοτήτων, για την προστασία από μη εξουσιοδοτημένη τροποποίησης/απώλεια/διαρροή/χρήση προσωπικών δεδομένων.

3. Πολιτική Διαχειρίσεως Χρηστών

- Υφίστανται κατάλληλα δικαιώματα προσβάσεως για κάθε ρόλο σύμφωνα με τις ανάγκες του ρόλου
- Υφίσταται τεκμηριωμένη πολιτική διαχειρίσεως χρηστών όπου μεταξύ άλλων καθορίζονται οι απαραίτητοι κανόνες ελέγχου προσβάσεως, τα δικαιώματα προσβάσεως και οι περιορισμοί για συγκεκριμένους ρόλους ανά χρήστη, σύμφωνα με τις διαδικασίες που σχετίζονται με τα προσωπικά δεδομένα.
- Είναι σαφώς καθορισμένος και καταγεγραμμένος ο διαχωρισμός των ρόλων ως προς τα δικαιώματα προσβάσεως (πχ. Αίτημα προσβάσεως, έγκριση προσβάσεως, διαχείριση προσβάσεως).
- Είναι σαφώς καθορισμένοι και καταγεγραμμένοι οι ρόλοι με αυξημένα δικαιώματα προσβάσεως, οι οποίοι έχουν εκχωρηθεί σε περιορισμένο αριθμό υπαλλήλων.

4. Διαχείριση Πόρων

- Ο Υπεύθυνος επεξεργασίας διατηρεί ενημερωμένο κατάλογο των πληροφοριακών πόρων που χρησιμοποιούνται για την επεξεργασία των προσωπικών δεδομένων (υλικό, λογισμικό και υποδομές δικτύου). Το αρχείο δύναται να περιλαμβάνει τουλάχιστον τις κάτωθι πληροφορίες: Πληροφοριακοί πόροι, τοποθεσία (φυσική ή ηλεκτρονική). Σε εξουσιοδοτημένο άτομο, έχει ανατεθεί το έργο της πρόσβασης, της τήρησης και επικαιροποίησης του εν λόγω καταλόγου.
- Οι πληροφοριακοί πόροι διαβαθμίζονται ως προς την κρισιμότητά τους και επιθεωρούνται σε περιοδική βάση.
- Οι ρόλοι και οι προσβάσεις στους πληροφοριακούς πόρους είναι καθορισμένοι και καταγεγραμμένοι.

5. Διαχείριση Αλλαγών

- Ο Υπεύθυνος Επεξεργασίας επιβεβαιώνει ότι όλες οι αλλαγές στο πληροφοριακό σύστημα είναι τεκμηριωμένες, εγκεκριμένες και επισκοπούνται αρμοδίως.
- Η ανάπτυξη του λογισμικού διενεργείται σε ειδικό ξεχωριστό περιβάλλον από το περιβάλλον παραγωγής. Όταν είναι απαραίτητος ο έλεγχος,

χρησιμοποιούνται εικονικά δεδομένα ή τεχνικές απομακρύνσεως ή τροποποιήσεως δεδομένων (data masking). Σε μεμονωμένες περιπτώσεις που αυτό δεν είναι εφικτό, συγκεκριμένες διαδικασίες λαμβάνουν χώρα για την προστασία των προσωπικών δεδομένων που χρησιμοποιούνται στον έλεγχο.

- Υφίσταται αναλυτική και καταγεγραμμένη πολιτική διαχειρίσεως αλλαγών, βάσει της οποίας τεκμηριώνονται οι αλλαγές, οι ρόλοι/χρήστες που έχουν δικαιώματα υλοποιήσεως αλλαγών και οι σχετικές εγκριτικές διαδικασίες. Η πολιτική διαχειρίσεως αλλαγών επικαιροποιείται σε περιοδική βάση.

6. Επεξεργασία προσωπικών δεδομένων

- Υφίστανται επίσημες οδηγίες και διαδικασίες για την επεξεργασία των προσωπικών δεδομένων με σκοπό την επίτευξη του κατάλληλου επιπέδου ασφαλείας πληροφοριών.
- Για κάθε περιστατικό ενδεχόμενης παραβίασης προσωπικών δεδομένων, ο Υπεύθυνος Επεξεργασίας ενημερώνει εντός 72 ωρών την Αρχή Προστασίας Προσωπικών Δεδομένων, σύμφωνα με τα οριζόμενα στο ΓΚΠΔ.
- Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων παρέχει επαρκή και τεκμηριωμένα στοιχεία της συμμόρφωσης με τον ΓΚΠΔ.

7. Διαχείριση περιστατικών ασφαλείας/προσωπικών δεδομένων

- Υφίσταται σχέδιο αντιμετωπίσεως περιστατικών ασφαλείας με αναλυτικές διαδικασίες με σκοπό την αποτελεσματική ανταπόκριση στα περιστατικά παραβιάσεως προσωπικών δεδομένων. Το εν λόγω σχέδιο περιέχει έναν κατάλογο με ενέργειες για τον περιορισμό των σχετικών κινδύνων καθώς και διακριτούς ρόλους και αρμοδιότητες των συμμετεχόντων στην εφαρμογή του.
- Υφίστανται διαδικασίες γνωστοποιήσεως για την αναφορά περιστατικών παραβιάσεως προσωπικών δεδομένων σύμφωνα με τον ΓΚΠΔ.

8. Επιχειρησιακή συνέχεια

- Ο εκτελών την επεξεργασία διαθέτει Σχέδιο Επιχειρησιακής Συνέχειας και Σχέδιο Ανακτήσεως Πληροφοριακών Συστημάτων από Καταστροφή (BCP/DRP) τα οποία είναι εγκεκριμένα από τη Διοίκηση και επιθεωρούνται ως προς την επάρκεια και αποτελεσματικότητα τους τουλάχιστον σε ετήσια βάση.

- Τα ανωτέρω σχέδια περιλαμβάνουν σαφείς δράσεις και ανάθεση σχετικών ρόλων και αρμοδιοτήτων.
- Υφίσταται κατάλληλές εναλλακτικές εγκαταστάσεις για την αποτελεσματική εφαρμογή των ανωτέρω σχεδίων.

9. Τήρηση εμπιστευτικότητας

- Ο Υπεύθυνος Επεξεργασίας διασφαλίζει ότι το προσωπικό κατανοεί τις ευθύνες και τις υποχρεώσεις που συνδέονται με την επεξεργασία προσωπικών δεδομένων. Οι ρόλοι και οι ευθύνες του προσωπικού γνωστοποιούνται σαφώς
- Πριν την ανάληψη των καθηκόντων τους οι εργαζόμενοι πρέπει να γνωρίζουν και να συμφωνούν με την πολιτική ασφάλειας του οργανισμού και την υπογραφή κατάλληλων συμβάσεων εμπιστευτικότητας.

10. Εκπαίδευση και ευαισθητοποίηση ασφαλείας πληροφοριών

- Ο Υπεύθυνος Επεξεργασίας διασφαλίζει την επαρκή πληροφόρηση όλου του προσωπικού σχετικά με τα μέτρα ασφαλείας στα πληροφοριακά συστήματα που σχετίζονται με την καθημερινή τους εργασία. Οι υπάλληλοι που σχετίζονται με θέματα επεξεργασίας προσωπικών δεδομένων είναι ενημερωμένοι και ευαισθητοποιημένοι σχετικά με θέματα προστασίας προσωπικών δεδομένων και τις ανάλογες υποχρεώσεις τους.
- Ο Υπεύθυνος Επεξεργασίας τηρεί κατάλληλα και εξειδικευμένα προγράμματα εκπαιδεύσεως και ευαισθητοποιήσεως ασφαλείας πληροφοριών (συμπεριλαμβανομένης της προστασίας των προσωπικών δεδομένων) για το προσωπικό
- Τα εκπαιδευτικά προγράμματα καθώς και τα προγράμματα ευαισθητοποιήσεως επικαιροποιούνται τουλάχιστον σε ετήσια βάση.

11. Διαχείριση κινδύνων ασφαλείας πληροφοριών

- Ο Υπεύθυνος Επεξεργασίας διενεργεί σε νέα κρίσιμα πληροφοριακά συστήματα / υπηρεσίες αξιολόγηση κινδύνων ασφαλείας πληροφοριών. Επιπλέον σε περιοδική βάση διενεργείται και επαναξιολόγηση κινδύνων ασφαλείας πληροφοριών σε υφιστάμενα κρίσιμα πληροφοριακά συστήματα / υπηρεσίες.

Β. Τεχνικά μέτρα

1. Έλεγχοι πρόσβασης/ταυτοποίησης

- Υφίστανται συστήματα ελεγχόμενης προσβάσεως των χρηστών στα πληροφοριακά συστήματα (περιλαμβάνοντας μεταξύ άλλων τη δημιουργία, την έγκριση, την αναθεώρηση και τη διαγραφή λογαριασμών χρηστών).
- Αποφεύγεται η χρήση κοινών λογαριασμών χρήστη.
- Υφίσταται κατάλληλος μηχανισμός ελέγχου προσβάσεως (ταυτοποιήσεως).
- Ο μηχανισμός ελέγχου πρόσβασης έχει τη δυνατότητα να ανιχνεύει και να μην επιτρέπει την χρήση των ασθενών κωδικών πρόσβασης (χωρίς υψηλό βαθμό πολυπλοκότητας).
- Υφίσταται κατάλληλη πολιτική κωδικών πρόσβασης. Η πολιτική ορίζει τουλάχιστον το μήκος του κωδικού πρόσβασης, την πολυπλοκότητα, την περίοδο ισχύος, καθώς επίσης και αριθμό αποδεκτών ανεπιτυχών προσπαθειών σύνδεσης.
- Οι κωδικοί πρόσβασης αποθηκεύονται σε κρυπτογραφημένη μορφή (hash).
- Ο έλεγχος ταυτοποίησης χρήστη δύο παραγόντων (2 factor authentication) πρέπει κατά προτίμηση να χρησιμοποιείται για πρόσβαση σε συστήματα που επεξεργάζονται προσωπικά δεδομένα.
- Οι κωδικοί προσβάσεως που δεν χρησιμοποιούνται για χρονική περίοδο τουλάχιστον έξι μηνών απενεργοποιούνται.

2. Αρχεία καταγραφής και παρακολούθησης

- Υφίστανται αρχεία καταγραφής δραστηριοτήτων σε κάθε σύστημα/εφαρμογή που χρησιμοποιείται για την επεξεργασία των προσωπικών δεδομένων, τα οποία περιλαμβάνουν όλους τους τύπους πρόσβασης στα εν λόγω δεδομένα (ανάγνωση, Τροποποίηση, Διαγραφή). Οι δραστηριότητες των χρηστών (συμπεριλαμβανομένων των διαχειριστών) οι οποίες μεταξύ άλλων περιλαμβάνουν την προσθήκη/διαγραφή/αλλαγή δικαιωμάτων των χρηστών καταγράφονται.
- Τα αρχεία καταγραφής προστατεύονται επαρκώς με κατάλληλα μέτρα ασφαλείας.
- Υφίσταται σύστημα παρακολούθησης των ανωτέρω αρχείων και σχετική ενημέρωση μέσω ειδοποιήσεων για ενδεχόμενα περιστατικά ασφαλείας.

3. Ασφάλεια βάσεων δεδομένων/εφαρμογών

- Στις βάσεις δεδομένων και στις εφαρμογές επεξεργάζονται τα προσωπικά δεδομένα που είναι άκρως απαραίτητα σύμφωνα με τους σκοπούς της επεξεργασίας.
- Κρυπτογράφηση υλοποιείται στα απαιτούμενα δεδομένα μέσω του λογισμικού/ή σχετικών μηχανισμών ασφαλείας.
- Υφίσταται κρυπτογράφηση στα αποθηκευτικά μέσα.
- Τεχνικές ψευδωνυμοποίησης ή ανωνυμοποίησης υλοποιούνται όπου απαιτείται.

4. Ασφάλεια τερματικών

- Οι χρήστες δεν έχουν τη δυνατότητα να απενεργοποιήσουν ή να παρακάμψουν τις ορισμένες ρυθμίσεις ασφάλειας.
- Οι χρήστες δεν έχουν προνόμια για να εγκαταστήσουν ή να απενεργοποιήσουν μη εξουσιοδοτημένες εφαρμογές λογισμικού.
- Υφίσταται κλείδωμα της οθόνης όταν ο χρήστης είναι ανενεργός για μια ορισμένη χρονική περίοδο.
- Οι κρίσιμες ενημερώσεις ασφαλείας που διατίθενται, εγκαθίστανται σε τακτά χρονικά διαστήματα.
- Δεν επιτρέπεται η μεταβίβαση των προσωπικών δεδομένων από σταθμούς εργασίας σε εξωτερικές συσκευές αποθήκευσης (π.χ. USB, DVD, εξωτερικούς σκληρούς δίσκους).

5. Ασφάλεια δικτύου/επικοινωνιών

- Στην κάθε πρόσβαση που πραγματοποιείται μέσω του Internet, η επικοινωνία είναι κρυπτογραφημένη μέσω κατάλληλων πρωτοκόλλων κρυπτογράφησης
- Η ασύρματη πρόσβαση στο σύστημα, επιτρέπεται μόνο για συγκεκριμένους χρήστες και διεργασίες οι οποίοι προστατεύονται μέσω μηχανισμών κρυπτογράφησης
- Η απομακρυσμένη πρόσβαση στα συστήματα αποφεύγεται. Σε περιπτώσεις όπου αυτό είναι απολύτως αναγκαίο, πρέπει να εκτελείται μόνο υπό τον έλεγχο και την παρακολούθηση του εξουσιοδοτημένου ατόμου από τον οργανισμό (π.χ. διαχειριστή /υπευθύνου ασφαλείας) μέσω προκαθορισμένων διατάξεων.
- Η κυκλοφορία προς και από τα πληροφοριακά συστήματα παρακολουθείται και ελέγχεται μέσω κατάλληλων μηχανισμών προστασίας firewalls και IDS/IPS.
- Υφίσταται κατάλληλος διαχωρισμός δικτύων

- Η πρόσβαση στα πληροφοριακά συστήματα λαμβάνει χώρα μόνο μέσω προ-εγκεκριμένου εξοπλισμού χρησιμοποιώντας τεχνικές όπως φιλτράρισμα MAC ή ελέγχου πρόσβασης στο δίκτυο (NAC).

6. Ασφάλεια από κακόβουλο λογισμικό

- Υφίσταται συνεχώς ενημερωμένη προστασία από κακόβουλο λογισμικό.

7. Αντίγραφα ασφαλείας

- Η δημιουργία αντιγράφων ασφαλείας και επαναφορά δεδομένων ορίζεται μέσω κατάλληλων τεκμηριωμένων διαδικασιών
- Στα Αντίγραφα Ασφαλείας παρέχεται το κατάλληλο επίπεδο της φυσικής και περιβαλλοντικής ασφαλείας σύμφωνα με τα υφιστάμενα των πρωτευόντων αρχείων.
- Η δημιουργία πλήρους αντιγράφου ασφαλείας, διενεργείται σε περιοδική βάση
- Οι διαδικασίες δημιουργίας αντιγράφων ασφαλείας δοκιμάζονται τακτικά
- Τα αντίγραφα ασφαλείας, αποθηκεύονται με ασφάλεια σε διαφορετικές τοποθεσίες από αυτές των πρωτευόντων.
- Τα αντίγραφα ασφαλείας όπου αυτό απαιτείται σύμφωνά με τη διαβάθμισή τους, είναι κρυπτογραφημένα.

8. Κινητές /φορητές συσκευές

- Υφίστανται διαδικασίες διαχείρισης για κινητές και φορητές συσκευές οι οποίες συμπεριλαμβάνουν σαφείς κανόνες ορθής χρήσης
- Οι συσκευές κινητών τηλεφώνων που επιτρέπεται να έχουν πρόσβαση σε προσωπικά δεδομένα και εταιρική πληροφορία είναι προ-εγγεγραμμένες και προ-εγκεκριμένες.
- Υφίστανται σαφείς ρόλοι και αρμοδιότητες όσον αφορά στις κινητές και φορητές συσκευές διαχείρισης
- Ο εκτελών την επεξεργασία δύναται να διαγράψει απομακρυσμένα τα προσωπικά δεδομένα (που σχετίζονται με την εργασία επεξεργασίας) σε φορητή συσκευή που έχει επηρεαστεί.
- Οι φορητές συσκευές, υποστηρίζουν τον διαχωρισμό της ιδιωτικής και επαγγελματικής χρήσης της συσκευής μέσω ασφαλούς εξειδικευμένου λογισμικού.
- Οι φορητές συσκευές προστατεύονται φυσικώς κατά της κλοπής, όταν δεν είναι σε χρήση.

- Υφίσταται έλεγχος ταυτοποίησης δύο παραγόντων για την πρόσβαση σε φορητές συσκευές .
- Τα προσωπικά δεδομένα που είναι αποθηκευμένα σε φορητές συσκευές είναι κρυπτογραφημένα.

9. Ασφάλεια κύκλου ζωής εφαρμογής

- Σύμφωνα με τις βέλτιστες πρακτικές, κατά την ανάπτυξη των εφαρμογών εφαρμογής, ακολουθούνται διεθνώς αποδεκτές αναγνωρισμένες πρακτικές, πλαίσια ή πρότυπα.
- Από τα αρχικά στάδια ανάπτυξης μιας εφαρμογής, καθορίζονται οι συγκεκριμένες απαιτήσεις ασφαλείας
- Υιοθετούνται, κατ' αναλογία με τις απαιτήσεις ασφαλείας, ειδικές τεχνολογίες και τεχνικές που έχουν σχεδιαστεί για την προστασία της ιδιωτικότητας και των δεδομένων.
- Κατά τη διάρκεια της ανάπτυξης, διεξάγονται οι απαιτούμενοι έλεγχοι για την τήρηση των αρχικών απαιτήσεων ασφαλείας.
- Πραγματοποιούνται οι απαραίτητοι έλεγχοι ασφαλείας (vulnerability assessments, penetration tests) πριν την ένταξη της εφαρμογής στις επιχειρησιακές διαδικασίες, ώστε να προχωρήσει η ένταξη της στο περιβάλλον παραγωγής.
- Διεξάγονται περιοδικοί τεχνικοί έλεγχοι ασφαλείας (vulnerability assessments, penetration tests), όπου αυτό κρίνεται βάσει των πολιτικών ασφαλείας απαραίτητο
- Πρέπει να λαμβάνεται ενημέρωση σχετικά με τις τεχνικές ευπάθειες των συστημάτων που χρησιμοποιούνται.
- Οι νέες εκδόσεις του λογισμικού ελέγχονται και να αξιολογούνται πριν εγκατασταθούν σε παραγωγικό περιβάλλον.

10. Διαγραφή δεδομένων / επαναχρησιμοποίηση

- Σε όλα τα μέσα με εμπιστευτική πληροφορία εκτελείται ασφαλής διαγραφή/απομαγνητισμός των δεδομένων, μέσω λογισμικού, πριν από την απόσυρσή τους. Σε περιπτώσεις όπου αυτό δεν είναι εφικτό (CD, DVD, κ.λπ.) πραγματοποιείται φυσική καταστροφή του μέσου.
- Διενεργείται ασφαλής καταστροφή των εγγράφων στα οποία υπήρχε αποθήκευση προσωπικών δεδομένων με χρήση καταστροφέα εγγράφων ή άλλης ασφαλούς μεθόδου.
- Όπου λαμβάνει χώρα η χρήση υπηρεσιών τρίτων μερών για την ασφαλή καταστροφή των μέσων ή των εγγράφων, πρέπει να υπάρχει συμφωνία

παροχής υπηρεσιών και σχετικά πρωτόκολλά καταστροφής με καταγραφή των αρχείων που καταστράφηκαν.

11. Φυσική Ασφάλεια

- Οι χώροι όπου έχουν εγκατασταθεί κρίσιμα συστήματα και υποδομές του πληροφοριακού συστήματος δεν είναι προσβάσιμοι από μη εξουσιοδοτημένο προσωπικό. Ορίζονται ζώνες ασφαλείας και προστατεύονται από κατάλληλους μηχανισμούς εισόδου. Τηρείται σε ασφαλές μέρος φυσικό ημερολόγιο ή ηλεκτρονικός έλεγχος όλων των προσβάσεων.
- Υφίστανται μέθοδοι σαφούς αναγνώρισης, μέσω κατάλληλων μέσων (π.χ. ειδικών ταυτοτήτων) για το σύνολο του προσωπικού και των επισκεπτών που έχουν πρόσβαση στις εγκαταστάσεις του εκτελούντος την επεξεργασία.
- Ορίζονται ζώνες ασφαλείας και προστατεύονται από κατάλληλους μηχανισμούς εισόδου. Τηρείται σε ασφαλές μέρος φυσικό ημερολόγιο ή ηλεκτρονικός έλεγχος όλων των προσβάσεων
- Τα συστήματα ανίχνευσης μη εξουσιοδοτημένης πρόσβασης εγκαθίστανται σε όλες τις ζώνες ασφαλείας.
- Υφίσταται αυτόματο σύστημα κατάσβεσης πυρκαγιάς, σύστημα κλιματισμού και σύστημα παροχής συνεχούς τροφοδοσίας (UPS)
- Το προσωπικό εξωτερικών συνεργατών έχει περιορισμένη και ελεγχόμενη πρόσβαση στις περιοχές με κρίσιμα συστήματα.
- Υπάρχουν κάμερες επιτήρησης (CCTV), στα σημεία που προβλέπεται από τις οδηγίες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.