Πολιτική Ασφάλειας Πληροφοριών

Συντάκτης Εγγράφου:
Υπ. ΣΔ T.B.S. s.a.

Έγκριση Εγγράφου:
Γενικός Δ/ντης T.B.S. s.a.

Περιεχόμενα

Εισαγωγή στην Ασφάλεια Πληροφοριών

Ορισμοί:

- Με τον όρο «**Ασφάλεια πληροφοριών**» εννοούμε την διατήρηση της εμπιστευτικότητας (confidentiality), ακεραιότητας (integrity), διαθεσιμότητας (availability) και προσβασιμότητας (accessibility) των πληροφοριών,
- Με τον όρο «**πληροφορίες**» εννοούμε κάθε στοιχείο / δεδομένο υφίσταται επεξεργασία στα συστήματα πληροφορικής της εταιρείας στα πλαίσια της δραστηριότητας της,
- Με τον όρο «**Επεξεργασία πληροφοριών**» (στοιχείων / δεδομένων) εννοούμε κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα ή σύνολα δεδομένων (περιλαμβανομένων των δεδομένου προσωπικού χαρακτήρα), όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή, η μεταβολή, η ανάκτηση, η αναζήτηση, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση, ο συνδυασμός, ο περιορισμός, η διαγραφή, η καταστροφή,
- Με τον όρο «**Συστήματα Πληροφορικής**» εννοούμε μεμονωμένα ή συνδυασμούς εξοπλισμού και λογισμικού που χρησιμοποιεί η εταιρεία για την επεξεργασία και τον διαμοιρασμό πληροφοριών.

Οι πληροφορίες που επεξεργάζεται η εταιρεία **T.B.S. s.a.** κατά την δραστηριοποίηση της θεωρούνται περιουσιακό στοιχείο υψίστης αξίας και ως εκ τούτου λαμβάνεται κάθε μέριμνα ώστε να προστατεύονται καθώς και τα Συστήματα Πληροφορικής που επιτρέπουν στην εταιρεία να επεξεργάζεται και να διαμοιράζεται τις πληροφορίες.

Στην εταιρεία **T.B.S. s.a.** έχει σχεδιαστεί και εφαρμόζεται ένα Σύστημα Διαχείρισης με σκοπό την αποτελεσματική διαχείριση και συνεχή βελτίωση του επιπέδου Ασφάλειας Πληροφοριών.

Κατά τον σχεδιασμό του εν λόγω Συστήματος Διαχείρισης λαμβάνονται υπόψη όλες οι νομοθετικές, κανονιστικές και συμβατικές υποχρεώσεις τις οποίες η Διοίκηση της εταιρείας δεσμεύεται να τηρεί.

Η Διοίκηση της **T.B.S. s.a.** δηλώνει την δέσμευση της να παρέχει όλους τους πόρους που απαιτούνται για την αποτελεσματική εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας των Πληροφοριών και την συνεχή βελτίωση της αποτελεσματικότητας του.

Η επίδοση της εταιρείας σχετικά με την Ασφάλεια των Πληροφοριών παρακολουθείται ανελλιπώς από την Διοίκηση στα πλαίσια της εφαρμογής του Συστήματος Διαχείρισης, μέσω της θέσπισης δεικτών αποτελεσματικότητας και αποδοτικότητας των διεργασιών και αντίστοιχων αντικειμενικών, μετρήσιμων στόχων για την Ασφάλεια των Πληροφοριών.

Η παρούσα Πολιτική Ασφάλειας των Πληροφοριών είναι δεσμευτική για όλο το προσωπικό και τους συνεργάτες της εταιρείας των οποίων η δραστηριότητα μπορεί να επηρεάσει την επίδοση της εταιρείας σχετικά με την Ασφάλεια των Πληροφοριών. Η Διοίκηση της **T.B.S. s.a.** εξασφαλίζει ότι κάθε μέλος του προσωπικού της και οι εξωτερικοί συνεργάτες λαμβάνουν γνώση και δεσμεύονται να τηρούν την εν λόγω Πολιτική.

Για την τήρηση των αρχών της παρούσας Πολιτικής Ασφάλειας των Πληροφοριών πρέπει να λαμβάνονται υπόψη και οι Διαδικασίες και Οδηγίες του Συστήματος Διαχείρισης καθώς και οι Περιγραφές Θέσης Εργασίας όπου καθορίζονται οι αρμοδιότητες των εμπλεκομένων για την ασφάλεια πληροφοριών**.**

Γενικές Αρχές

Γενικά Σημεία

- Η Ασφάλεια των Πληροφοριών είναι αρμοδιότητα όλων.
- Το σύστημα πληροφορικής της **T.B.S. s.a.** παρέχεται αποκλειστικά για χρήση που σχετίζεται με τις δραστηριότητες της εταιρείας.
- Χρήση του συστήματος πληροφορικής της **T.B.S. s.a.** για προσωπικούς λόγους (συμπεριλαμβανομένων e-mail και του διαδικτύου) απαγορεύεται. Δεν πρέπει να υπάρχουν προσδοκίες ιδιωτικότητας όταν κάποιος χρησιμοποιεί το σύστημα πληροφορικής της **T.B.S. s.a.**
- η **T.B.S. s.a.** διατηρεί το δικαίωμα να παρακολουθεί κάθε πτυχή του συστήματος πληροφορικής με σκοπό να προστατέψει τα νόμιμα επιχειρηματικά της δικαιώματα. Οι πληροφορίες που συλλέγονται από κάθε παρακολούθηση μπορεί να χρησιμοποιηθούν για να κινήσουν ή να υποστηρίξουν πειθαρχικές διαδικασίες.
- Παραβίαση των όρων της παρούσας πολιτικής έχει ως αποτέλεσμα πειθαρχικές ενέργειες οι οποίες, ανάλογα με την σοβαρότητα της παραβίασης, μπορεί να συμπεριλαμβάνουν:
  - Προφορική σύσταση / προειδοποίηση από την Διοίκηση,
  - Επίσημη γραπτή σύσταση / προειδοποίηση για σοβαρό παράπτωμα,
  - Απόλυση λόγω σοβαρού παραπτώματος,
  - Ποινικές διαδικασίες,
  - Αστικές διαδικασίες για την αποκατάσταση των ζημιών.
- Στο διαδίκτυο διακινούνται πληροφορίες και υλικό το οποίο συχνά περιγράφεται με τον όρο «***στοιχεία τα οποία άλλοι μπορεί να θεωρούν προσβλητικά***» και χρησιμοποιείται συχνά από κακοποιά στοιχεία για παγίδευση χρηστών του διαδικτύου με απώτερο σκοπό την προσβολή συστημάτων από κακόβουλων λογισμικό. Ο όρος αυτός συμπεριλαμβάνει αλλά δεν περιορίζεται σε:
  - Πορνογραφικό ή σεξουαλικό υλικό,
  - Ρατσιστικό, σεξιστικό ή ομοφοβικό υλικό,
  - Αναφορές θρησκευτικού / πολιτικού περιεχομένου,
  - Αντιαισθητικό / αντικοινωνικό υλικό (όπως βανδαλισμοί, άσκηση βίας σε ανθρώπους ή ζώα).

  Προσπέλαση ιστοσελίδων με περιεχόμενο αυτού του είδους απαγορεύεται αυστηρά να γίνεται μέσω του δικτύου ή με χρήση εξοπλισμού που ανήκει στο σύστημα πληροφορικής της εταιρείας **(αποτελεί ενέργεια υψηλού κινδύνου για την ασφάλεια πληροφοριών).**

Ενέργειες για την συμμόρφωση

- ✓ Συνετή, προσεκτική και λελογισμένη χρήση των συστημάτων πληροφορικής,
- ✓ Άμεση αναφορά κάθε περιστατικού ή υπόνοια περιστατικού το σχετικό με την ασφάλεια των πληροφοριών ή των εγκαταστάσεων στον Υπ. ΣΔ.

Αρχές ορθής διαχείρισης Λειτουργιών και Επικοινωνιών

1. Διαδικασίες Τυποποιημένης Λειτουργίας

Γενικά Σημεία

- Στην **T.B.S. s.a.** εφαρμόζονται διαδικασίες τυποποιημένης λειτουργίας για την καθημερινή συντήρηση των συστημάτων πληροφορικής και των υποδομών της με σκοπό να διασφαλιστεί η υψηλότερη δυνατή διαθεσιμότητα και επίδοση των συστημάτων αυτών.
- Αλλαγές στα συστήματα πληροφορικής της εταιρείας υλοποιούνται με ελεγχόμενο τρόπο για την αποτελεσματική διαχείριση αλλαγών.
- Τα αναπτυξιακά και δοκιμαστικά περιβάλλοντα λειτουργίας των συστημάτων και των εφαρμογών διατηρούνται πάντα ξεχωριστά από το ζωντανό λειτουργικό περιβάλλον για τη μείωση κινδύνου τυχαίων αλλαγών ή μη εξουσιοδοτημένης πρόσβασης.

Ενέργειες για την συμμόρφωση

- ✓ Έκδοση και εφαρμογή κατάλληλων διαδικασιών / οδηγιών τυποποιημένης λειτουργίας,
- ✓ Αξιολόγηση όλων των σημαντικών αλλαγών στα συστήματα πληροφορικής και στην κύρια υποδομή για την επίπτωσή τους στην ασφάλεια πληροφοριών (αναπόσπαστο μέρος της τυπικής αξιολόγησης κινδύνου),
- ✓ Διαχωρισμός του λειτουργικού περιβάλλοντος και του περιβάλλοντος ανάπτυξης / δοκιμών με κατάλληλα μέσα ελέγχους, συμπεριλαμβανομένων των ακόλουθων:
  - Εκτέλεση σε ξεχωριστούς υπολογιστές, domains και δίκτυα,
  - Διαφορετικά usernames και κωδικοί,
  - Χρήση εικονικών δεδομένων και πληροφοριών κατά τις δοκιμές – ελέγχους,
  - Ανάθεση σε στελέχη που είναι ικανά να αξιολογήσουν και να δοκιμάσουν λειτουργικά συστήματα.

2. Σχεδιασμός και αποδοχή συστημάτων πληροφορικής

Γενικά Σημεία

- Όλα τα συστατικά μέρη και τα χαρακτηριστικά του εξοπλισμού και της υποδομής συστημάτων πληροφορικής της **T.B.S. s.a.** λαμβάνονται υπόψη κατά την κατάρτιση του ετήσιου προϋπολογισμού της εταιρείας και παρέχονται οι απαραίτητοι πόροι για την προμήθεια, συντήρηση, αντικατάσταση τους έτσι ώστε να προσαρμόζονται πάντα στις απαιτήσεις με βάση τον φόρτο εργασιών και τις λειτουργικές ανάγκες της εταιρείας.
- Ως σημαντικά συστατικά μέρη και τα χαρακτηριστικά του εξοπλισμού και της υποδομής συστημάτων πληροφορικής ενδεικτικά αναφέρονται τα παρακάτω:
  - File servers,
  - Domain servers,
  - E-mail servers,

- Web servers,
- Εκτυπωτές,
- Δίκτυα,
- Υποστηρικτικός εξοπλισμός (CCTV, Access Control, Server room κ.ά.).

Ενέργειες για την συμμόρφωση

- ✓ Όλα τα τμήματα πρέπει να ενημερώνουν τον Γενικό Δ/ντη για τις απαιτήσεις νέου εξοπλισμού / συστημάτων ή αναβάθμισης, ή βελτιώσεις που απαιτούνται για τα υπάρχοντα συστήματα,
- ✓ Για την προμήθεια κάθε νέου εξοπλισμού / συστήματος εφαρμόζεται η σχετική διαδικασία τυποποιημένης λειτουργίας του συστήματος διαχείρισης μετά από έγκριση του Γενικού Δ/ντη,
- ✓ Νέα πληροφοριακά συστήματα, αναβαθμίσεις υπηρεσιών, patches κ.α. πρέπει να υποβάλλονται σε κατάλληλο έλεγχο από τον Υπ. Μηχανογράφησης πριν την αποδοχή και εφαρμογή τους σε ζωντανό περιβάλλον,
- ✓ Τα κριτήρια αποδοχής πρέπει να προσδιορίζονται σαφώς και να καταγράφονται και να συμφωνούνται με τον προμηθευτή,
- ✓ Σημαντικές αναβαθμίσεις του συστήματος πρέπει να ελέγχονται διεξοδικά παράλληλα με το υπάρχον σύστημα σε ένα ασφαλές περιβάλλον δοκιμών.

3. Προστασία από Κακόβουλο Λογισμικό (Malicious and Mobile Code)

Γενικά Σημεία

- Στην εταιρεία **T.B.S. s.a.** λαμβάνονται όλα τα κατάλληλα μέτρα για την προστασία των συστημάτων και υποδομών πληροφορικής καθώς και των πληροφοριών και δεδομένων που αυτά επεξεργάζονται, έναντι Κακόβουλου Λογισμικού,
- Η λειτουργία των συστημάτων πληροφορικής είναι πάντα υπό ενεργοποιημένο κατάλληλο και ενημερωμένο λογισμικό προστασίας από ιούς σε όλους τους servers και υπολογιστές,
- Με σκοπό την αποτροπή του κακόβουλου λογισμικού, διεξάγονται κατάλληλοι έλεγχοι πρόσβασης (πχ. Δικαιώματα διαχειριστή, χρήστη) για την αποτροπή εγκατάστασης λογισμικού από όλους τους χρήστες,
- Κακόβουλο Λογισμικό (Malicious and Mobile Code) παρουσιάζεται σε νέες τεχνολογίες και εφαρμογές οι οποίες συχνά βρίσκονται στις ιστοσελίδες, στα emails, και περιλαμβάνονται (ενδεικτικά αναφέρονται) σε:
  - ActiveX,
  - Java,
  - JavaScript,
  - VBScript,
  - Macros,
  - HTTPS,

- HTML.

Ενέργειες για την συμμόρφωση

- ✓ Το προσωπικό και οι εξωτερικοί συνεργάτες της εταιρείας έχουν υποχρέωση:
  - να μην επιτρέπουν την εμφάνιση καταστάσεων από τις οποίες μπορεί να προέλθει προσβολή του συστήματος πληροφορικής της εταιρείας από Κακόβουλο Λογισμικό εφαρμόζοντας πιστά τις σχετικές Διαδικασίες / Οδηγίες τυποποιημένης λειτουργίας,
  - σε περίπτωση που εντοπίζουν ή υποπτεύονται προσβολή από Κακόβουλο Λογισμικό στο σύστημα πληροφορικής ή σε αποθηκευτικό μέσο της εταιρείας πρέπει να ενημερώσει άμεσα τον Υπ. Μηχανογράφησης και σε απουσία του τον Γενικό Δ/ντη ή τον Υπ. ΣΔ.
- ✓ Patches λογισμικού εφαρμόζονται κατάλληλα σε όλα τα λογισμικά του δικτύου του οργανισμού και να υπάρχει μία πλήρης καταγραφή των ποια patches έχουν εφαρμοστεί και πότε,
- ✓ Αιτήματα για εγκατάσταση λογισμικού πρέπει να γίνονται αποδεκτά μόνο όταν υπάρχει τεχνική επιβεβαίωση από τον Υπ. Μηχανογράφησης,
- ✓ Κατάλληλο και ενημερωμένο λογισμικό προστασίας από Κακόβουλο Λογισμικό πρέπει να εγκαθίσταται σε κατάλληλα σημεία του δικτύου (σταθερό και κινητό εξοπλισμό) και σε εξοπλισμό επισκεπτών που τυχόν συνδέεται στο δίκτυο της εταιρείας.

4. Αντίγραφα Ασφαλείας (Backups)

Γενικά Σημεία

- Στην εταιρεία **T.B.S. s.a.** λαμβάνονται τακτικά αντίγραφα ασφαλείας των πληροφοριών που επεξεργάζεται η επιχείρηση, για τη διασφάλιση ότι η λειτουργία μπορεί να ανακάμψει αποτελεσματικά μετά από κάποια καταστροφή, αποτυχία μέσου ή σφάλμα,
- Αντίγραφα ασφαλείας λαμβάνονται βάσει καθορισμένης συχνότητας και εξασφαλίζεται πλήρης τεκμηρίωση της λήψης εφεδρικών αντιγράφων τα οποία φυλάσσονται σε ασφαλές χώρο και εκτός των εγκαταστάσεων,
- Στα πλαίσια της σύμβασης συνεργασίας με οποιοδήποτε 3ο μέρος (π.χ. εξωτερικοί συνεργάτες, πελάτες) που επεξεργάζεται πληροφορίες, εξασφαλίζεται ότι τηρείται ο ενδεδειγμένος τρόπος λήψης εφεδρικών αντιγράφων.

Ενέργειες για την συμμόρφωση

- ✓ Διασφάλιση ότι η απομακρυσμένη τοποθεσία είναι αρκετά μακριά ώστε να αποφευχθεί η επίδρασή του από όποια καταστροφή προκύψει στο κύριο χώρο.
- ✓ Εκτέλεση τακτικών ασκήσεων ανάκτησης αποθηκευμένων πληροφοριών από τα εφεδρικά μέσα αντιγράφων ασφαλείας για τη διασφάλιση της αξιοπιστίας των μέσων και της διαδικασίας αποθήκευσης (κατ'ελάχιστον ετησίως και όποτε άλλοτε κρίνεται απαραίτητο από τον Υπ. Μηχανογράφησης π.χ. μετά από μια σημαντική αλλαγή στο σύστημα ή μετά από ένα περιστατικό ασφάλειας, με τήρηση αρχείου όπου αναφέρεται το αποτέλεσμα της άσκησης).

5. Χειρισμός Μέσων Αποθήκευσης (ηλεκτρονικά και έντυπα)

Γενικά Σημεία

- Τα ηλεκτρονικά μέσα αποθήκευσης που επιτρέπεται να συνδεθούν στο δίκτυο της εταιρείας **T.B.S. s.a.** είναι:
  - Σκληροί δίσκοι υπολογιστών (εσωτερικοί και εξωτερικοί),
  - CD,
  - DVD,
  - Οπτικοί δίσκοι - Optical Disks,
  - Ψηφιακές Κάμερες.
- Τα αφαιρούμενα μέσα αποθήκευσης επί υπολογιστών (πχ. δίσκοι) προστατεύονται για να αποφευχθεί η ζημιά, κλοπή ή μη εξουσιοδοτημένη πρόσβαση,
- Τα ηλεκτρονικά μέσα αποθήκευσης που μεταφέρονται προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, λανθασμένη χρήση ή διακοπή,
- Η τεκμηρίωση του συστήματος (έγγραφα και αρχεία) προστατεύεται από μη εξουσιοδοτημένη πρόσβαση. Παραδείγματα των εγγράφων που προστατεύονται συμπεριλαμβάνουν, αλλά δεν περιορίζονται:
  - Αρχεία και τεκμηρίωση σχετικά με τις εφαρμογές και τα προγράμματα που είναι εγκατεστημένα στο δίκτυο,
  - Διαδικασίες / Οδηγίες τυποποιημένης λειτουργίας και τα συνοδευτικά τους έγγραφα / έντυπα,
  - Διεργασίες,
  - Αρχεία και τεκμηρίωση σχετικά με την δομή του δικτύου και την οργάνωση βάσεων δεδομένων, φακέλων και άλλων στοιχείων του δικτύου,
  - Αρχεία και τεκμηρίωση σχετικά με λεπτομέρειες εξουσιοδότησης και δικαιώματα πρόσβασης,

Ενέργειες για την συμμόρφωση

- ✓ Η πρόσβαση στα ηλεκτρονικά μέσα αποθήκευσης και στα έγγραφα του Συστήματος Διαχείρισης είναι ελεγχόμενη αυστηρά μόνο για κατάλληλα εξουσιοδοτημένα πρόσωπα.
- ✓ Διαγραφή κατά τρόπο μη αντιστρέψιμο κάθε πληροφορίας από τα ηλεκτρονικά μέσα αποθήκευσης που μεταφέρονται εκτός εταιρείας για επισκευή και τήρηση αρχείου από όπου προκύπτουν η ημερομηνία και ώρα αποστολής / παραλαβής, οι υπεύθυνοι αποστολής / παραλαβής, ο προορισμός και η αιτία της μεταφοράς. Αν αυτό δεν είναι εφικτό τα αποθηκευτικά μέσα δεν μεταφέρονται εκτός εταιρείας για επισκευή και αντικαθίστανται με άλλα αφού καταστραφούν με μηχανικό τρόπο (τρυπάνι) και τηρηθεί πρωτόκολλο καταστροφής.
- ✓ Αρχείο όλης της έγγραφης τεκμηρίωσης λήψης των αντιγράφων ασφαλείας, αντίγραφο της διαδικασίας ανάκαμψης καθώς και μία πλήρης καταχώρηση των πληροφοριών όλου του συστήματος σε εφεδρικό σκληρό δίσκο φυλάσσεται ανά πάσα στιγμή σε μία ασφαλή τοποθεσία εκτός του χώρου της εταιρείας με επιπλέον αντίγραφο στον κύριο χώρο.

- ✓ Για την απόρριψη άχρηστων / αποσυρόμενων εγγράφων χρησιμοποιείται κάδος ανακύκλωσης του δήμου αφού έχει προηγηθεί καταστροφή με τεμαχιστικό μηχάνημα (shredder) κάθε εγγράφου που απορρίπτεται και τηρηθεί πρωτόκολλο καταστροφής.

6. Παρακολούθηση

Γενικά Σημεία

- Στην εταιρεία **T.B.S. s.a.** για την επίτευξη της ασφάλειας και για την διευκόλυνση της διερεύνησης περιστατικών εφαρμόζονται τεχνικές παρακολούθησης. Στην περίπτωση αυτή τα αρχεία καταγραφής ελέγχου (audit logs) περιέχουν κατ' ελάχιστο τις ακόλουθες πληροφορίες:
  - Ταυτότητα συστήματος (System identity),
  - Όνομα χρήστη,
  - Επιτυχής/Ανεπιτυχής είσοδος,
  - Επιτυχής/Ανεπιτυχής έξοδος.

Ενέργειες για την συμμόρφωση

- ✓ Διατήρηση audit logs για τουλάχιστον 6 μήνες που καταγράφουν τις εξαιρέσεις και άλλα περιστατικά σχετικά με την ασφάλεια,
- ✓ Προστασία των audit logs από μη εξουσιοδοτημένη πρόσβαση,
- ✓ Τήρηση αρχείου δραστηριοτήτων για το λειτουργικό προσωπικό και τους διαχειριστές συστήματος που περιλαμβάνει:
  - Back-up timings και στοιχεία (ημερομηνία / ώρα / χρήστης) αλλαγής των ηλεκτρονικών μέσων λήψης εφεδρικών αντιγράφων xchange of backup tapes,
  - System event start και System finish times και στοιχεία εμπλεκομένων χρηστών,
  - System errors (περιγραφή, ημερομηνία, ώρα) και διορθωτικές ενέργειες που έγιναν.
- ✓ Τακτικός έλεγχος της ορθής τήρησης audit logs από εξουσιοδοτημένο πρόσωπο (τουλάχιστον εξαμηνιαίως με τήρηση αρχείου όπου αναφέρονται τα αποτελέσματα του ελέγχου καθώς και το αν υπήρξαν περιστατικά ή παρολίγον ασφάλειας πληροφοριών),
- ✓ Συγχρονισμός σε ετήσια βάση όλων των ρολογιών των υπολογιστών πρέπει με την προέλευση της ώρας GSI για να διασφαλιστεί η ακρίβεια όλων των αρχείων καταγραφής ελέγχου των συστημάτων και η διερεύνηση τυχόν περιστατικών ασφάλειας.

7. Διαχείριση Δικτύου

Γενικά Σημεία

- Στην εταιρεία **T.B.S. s.a.** η διαχείριση του δικτύου θεωρείται κρίσιμος παράγοντας για την εύρυθμη και ασφαλή λειτουργία,
- Συνδέσεις στο δίκτυο της εταιρείας γίνονται με ελεγχόμενο τρόπο,
- Ασύρματα δίκτυα λειτουργούν με αυξημένο έλεγχο πρόσβασης μόνο για το προσωπικό της εταιρείας και για κατάλληλα εξουσιοδοτημένους εξωτερικούς συνεργάτες,

Ενέργειες για την συμμόρφωση

- ✓ Έκδοση και εφαρμογή διαδικασιών / οδηγιών με ξεκάθαρες αρμοδιότητες και ενέργειες για τη διαχείριση και ορθή χρήση του σταθερού και κινητού εξοπλισμού,
- ✓ Τεκμηρίωση της αρχιτεκτονικής και όλων των μερών του δικτύου και των στοιχείων εξοπλισμού που απαρτίζουν το σύστημα πληροφορικής και αποθήκευσή της τεκμηρίωσης με ρυθμίσεις διαμόρφωσης όλων των μερών υλικού και λογισμικού που απαρτίζουν το δίκτυο (κατάλογος που ανανεώνεται όταν προστίθενται ή αφαιρούνται περιουσιακά στοιχεία),
- ✓ Το σύστημα πληροφορικής προστατεύεται από UPS για τη μείωση του κινδύνου βλάβης ή απώλειας πληροφοριών από διαταραχές τάσης τροφοδοσίας του δικτύου ηλεκτροδότησης,
- ✓ Καλώδια που μεταφέρουν δεδομένα ή υποστηρίζουν σημαντικές υπηρεσίες πληροφοριών προστατεύονται από υποκλοπές ή ζημίες,
- ✓ Τα καλώδια ρεύματος διαχωρίζονται κατά την όδευσης τους από τα καλώδια δικτύου για την αποφυγή παρεμβολών,
- ✓ Τα καλώδια δικτύου προστατεύονται από κανάλι όδευσης και αποφεύγονται οι διαδρομές μέσω περιοχών όπου υπάρχει ελεύθερη πρόσβαση,
- ✓ Χρήση μεθόδων και τεχνικών κρυπτογράφησης για την προστασία των δεδομένων που διακινούνται στο δίκτυο,
- ✓ Διασφάλιση ότι όλοι οι hosts έχουν ικανοποιητικό επίπεδο ασφαλείας,
- ✓ Επανεξέταση σε 6μηνιαία βάση των υπηρεσιών δικτύου των λειτουργικών συστημάτων και απενεργοποίηση όλων των υπηρεσιών που δεν χρειάζονται,
- ✓ Χρήση κρυπτογράφησης στα ασύρματα δίκτυα για την αποφυγή διακοπής των πληροφοριών (WPA2 κατ' ελάχιστο).

8. Ασφάλεια πληροφοριών σε σχέσεις με εξωτερικούς παρόχους

Γενικά Σημεία

- Η εταιρεία **T.B.S. s.a.** για την κάλυψη αναγκών σε εξοπλισμό, είδη ή υπηρεσίες που μπορούν να επιδράσουν στην ασφάλεια των πληροφοριών που διαχειρίζεται (π.χ. μηχανογραφική υποστήριξη, νομική υποστήριξη, εξοπλισμός μηχανογράφησης και τηλεπικοινωνιών, φύλαξη, ταχυδρομικές υπηρεσίες, ενοικίαση χώρων) μπορεί να απευθύνεται σε εξωτ. Παρόχους,
- Πριν από κάθε συνεργασία αυτού του είδους η εταιρεία προσδιορίζει τις απαιτήσεις έτσι ώστε να μετριάζεται ο κίνδυνος για την ασφάλεια των πληροφοριών από την πρόσβαση του εξωτ. παρόχου στις πληροφορίες,
- Οι απαιτήσεις αυτές συμφωνούνται με τον εξωτ. πάροχο και η ικανοποίησή τους παρακολουθείται στα πλαίσια συμβάσεων συνεργασίας μέσω των οποίων προσδιορίζονται:
  - Η έννοια της ασφάλειας (availability, accessibility, integrity, confidentiality), οι απαιτήσεις ασφάλειας και το επίπεδο ασφάλειας που πρέπει να εξασφαλίζεται (classification),
  - Τα ακριβή χαρακτηριστικά του εξοπλισμού / λογισμικού / υπηρεσιών και τα κριτήρια αποδοχής,

- Οι πληροφορίες στις οποίες θα έχει πρόσβαση ο εξωτ. πάροχος και το είδος, μεθοδολογία, διάρκεια της πρόσβασης συμπεριλαμβανομένων των απαιτήσεων για απομακρυσμένη πρόσβαση,
- Η υποχρέωση του εξωτ. παρόχου να προστατεύει τις πληροφορίες της εταιρείας στις οποίες έχει πρόσβαση και να συμμορφώνεται με τις προβλέψεις της παρούσας Πολιτικής και των απαιτήσεων ασφάλειας που απορρέουν από αυτή,
- Οι κανόνες αποδεκτής και μη αποδεκτής χρήσης των πληροφοριών,
- τα μέτρα αντιμετώπισης του κινδύνου που πρέπει να λαμβάνει ο εξωτ. Πάροχος και το πως επιβάλλεται η λήψη των μέτρων αυτών,
- Οι έλεγχοι που πρέπει να γίνονται για να επαληθεύεται ανά πάσα στιγμή η διατήρηση της ασφάλειας των πληροφοριών, συμπεριλαμβανομένου του δικαιώματος της εταιρείας να διενεργεί επιθεωρήσεις των διεργασιών και των μέτρων ελέγχου που εφαρμόζονται για την προμήθεια / συνεργασία,
- Οι διαδικασίες αντιμετώπισης περιστατικών απώλειας της ασφάλειας των πληροφοριών και προβλέψεις για αντιμετώπιση εκτάκτων αναγκών, με έμφαση στις απαιτήσεις της νομοθεσίας περί γνωστοποιήσεων / ενημερώσεων και συνεργασίας μεταξύ εταιρείας και προμηθευτή σε καταστάσεις εκτάκτου ανάγκης ή αντιμετώπισης περιστατικών ασφάλειας πληροφοριών,
- Η διαδικασία χειρισμού περίπτωσης παράδοσης εκ μέρους του εξωτ. παρόχου προϊόντος ή υπηρεσίας μη συμμορφούμενη προς τις συμφωνημένες απαιτήσεις,
- Οι απαιτήσεις για τις υποδομές και εγκαταστάσεις της εταιρείας που θα πρέπει να αξιοποιηθούν κατά την προμήθεια / συνεργασία καθώς και οι απαιτήσεις εκπαίδευσης, γνώσεων και εμπειρίας που πρέπει να ικανοποιεί το προσωπικό της εταιρείας που θα εμπλακεί στην υλοποίηση,
- Τα στοιχεία ταυτότητας του προσωπικού του εξωτ. παρόχου που είναι εξουσιοδοτημένο να έχει πρόσβαση στις πληροφορίες ή οι απαιτήσεις εξουσιοδότησης του προσωπικού και τυχόν απαιτήσεις για επαλήθευση σπουδών, γνώσεων, πρότερης εργασιακής εμπειρίας, διαγωγής,
- Προβλέψεις σχετικά με την δυνατότητα του εξωτ. παρόχου να αναθέσει υπεργολαβικά σε άλλο μέρος ένα τμήμα ή το σύνολο της προμήθειας / παροχής της υπηρεσίας και τις προϋποθέσεις που θα ισχύουν για αυτό,
- Οι απαιτήσεις για την ανταλλαγή πληροφοριών και οι προβλέψεις για την διατήρηση της ασφάλειας των πληροφοριών κατά την διάρκεια της μεταφοράς,
- Οι νομοθετικές και κανονιστικές απαιτήσεις (προστασίας δεδομένων, προστασίας πνευματικής ιδιοκτησίας) και περιγραφή του πως ικανοποιούνται οι απαιτήσεις,
- Την αποδοχή του εξωτ. παρόχου να υποβάλλει αν αυτό απαιτείται περιοδικές αναφορές σχετικά με την αποτελεσματικότητα των μέτρων.

Ενέργειες για την συμμόρφωση

✓ Σύναψη συμβάσεων συνεργασίας με προμηθευτές προϊόντων και υπηρεσιών που επηρεάζουν την επίδοση της εταιρείας σχετικά με την ασφάλεια των πληροφοριών.

9. Ετήσιος Έλεγχος Κατάστασης

Γενικά Σημεία

- Κατά την δραστηριοποίηση της εταιρείας **T.B.S. s.a.** το σύστημα πληροφορικής, η επάρκεια των πόρων και των τεχνικών και οργανωτικών μέτρων αντιμετώπισης των κινδύνων και γενικά η επάρκεια και αποτελεσματικότητα του συστήματος για την υποστήριξη των δραστηριοτήτων της εταιρείας, ελέγχεται τακτικά και προσαρμόζεται κατάλληλα.

Ενέργειες για την συμμόρφωση

✓ Σε ετήσια βάση διεξάγεται με ευθύνη του Υπ. Μηχανογράφησης εσωτερικός έλεγχος της κατάστασης όλων των συστημάτων και υποδομών IT του οργανισμού που περιλαμβάνει, αλλά δεν περιορίζεται, τα ακόλουθα:

- Ένα πλήρες τεστ διείσδυσης,
- Μία σύνοψη δικτύου που θα προσδιορίζει όλες τις διευθυνσιοδοτημένες συσκευές με IP,
- Μία ανάλυση δικτύου, συμπεριλαμβανομένων exploitable switches και gateways,
- Ανάλυση ευπαθειών (vulnerability analysis), συμπεριλαμβανομένων patch levels, μη ασφαλής κωδικούς και των υπηρεσιών που χρησιμοποιούνται),
- Ανάλυση εκμετάλλευσης (Exploitation analysis),
- Μία αναλυτική αναφορά με προτάσεις για βελτίωση.

10. Ασφαλείς Περιοχές

Γενικά Σημεία

- Η Διοίκηση της **T.B.S. s.a.** λαμβάνει ειδική μέριμνα για την ασφάλεια των χώρων που στεγάζονται οι δραστηριότητες της εταιρείας. Το κατάλληλο επίπεδο προστασίας για την ασφάλεια των χώρων προσδιορίζεται μέσω εκτενούς αξιολόγησης κινδύνων,
- Η μέριμνα για προστασία από μη εξουσιοδοτημένη πρόσβαση ατόμων στους χώρους ξεκινάει από τα γραφεία που στεγάζεται η εταιρεία και επεκτείνεται σε όλο το κτήριο με αξιολόγηση της ευπάθειας του κτηρίου και της περιμέτρου αλλά και της τοποθεσίας που βρίσκεται το κτήριο.

Ενέργειες για την συμμόρφωση

✓ Έκδοση και εφαρμογή διαδικασιών / οδηγιών με ξεκάθαρες αρμοδιότητες και ενέργειες για την ασφάλεια των χώρων της εταιρείας και για τη διαχείριση της πρόσβασης στους χώρους,

✓ Το κτήριο διαθέτει **κατάλληλους** μηχανισμούς ελέγχου της πρόσβασης που περιλαμβάνουν τα ακόλουθα:

- Τοποθέτηση μηχανισμών ελέγχου πρόσβασης στην κύρια είσοδο του γραφείου,
- Κλειδωμένες πόρτες και παράθυρα εκτός των εργάσιμων ωρών,
- Τοποθέτηση συστήματος ανίχνευσης εισβολής και συναγερμού που ενεργοποιείται εκτός των εργάσιμων ωρών,
- Τοποθέτηση συστήματος κλειστού κυκλώματος καμερών παρακολούθησης (CCTV),
- Τοποθέτηση συστήματος προστασίας κατά των καταστροφών (π.χ. φωτιά, βανδαλισμό),

- ✓ Τήρηση αρχείου εισόδου – εξόδου κάθε ατόμου στις προστατευόμενες περιοχές (π.χ. server room),
- ✓ Κάθε επισκέπτης της εταιρείας καταγράφεται στο βιβλίο επισκεπτών, από την άφιξη του μέχρι την αποχώρηση και καθ'όλη την διάρκεια της επίσκεψης του επιτηρείται από ένα υπάλληλο του οργανισμού ο οποίος αναφέρεται στο βιβλίο επισκεπτών,
- ✓ Τα κλειδιά όλων των προστατευόμενων περιοχών και των περιοχών που έχουν εξοπλισμό τoy συστήματος πληροφορικής φυλάσσονται κεντρικά από τον Γενικό Δ/ντη,
- ✓ Παραμονή προσωπικού, εξωτερικών συνεργατών ή επισκεπτών στους χώρους της εταιρείας εκτός ωρών εργασίας απαγορεύεται χωρίς την έγκριση του Γενικού Δ/ντη ή του προϊστάμενου του τμήματος όπου ανήκει ο εργαζόμενος ή με το οποίο συνεργάζεται ο εξωτερικός συνεργάτης.

11. Ασφάλεια Εγγράφων και Εξοπλισμού

Γενικά Σημεία

- Η Διοίκηση της **T.B.S. s.a.** λαμβάνει ειδική μέριμνα για την ασφάλεια των εγγράφων και του εξοπλισμού μέσω των οποίων γίνεται η επεξεργασία των πληροφοριών. Το κατάλληλο επίπεδο προστασίας για την ασφάλεια εγγράφων και εξοπλισμού προσδιορίζεται μέσω εκτενούς αξιολόγησης κινδύνων,
- Για να επιτραπεί η πρόσβαση σε έγγραφα ή εξοπλισμό που χρησιμοποιείται για την επεξεργασία πληροφοριών απαιτείται εκχώρηση κατάλληλης εξουσιοδότησης ή/και χαρακτηρισμός του επιπέδου προστασίας που πρέπει να απολαμβάνουν οι πληροφορίες (classification).

Ενέργειες για την συμμόρφωση

- ✓ Τα έγγραφα σε ένα ανοιχτό γραφείο προστατεύονται ανάλογα με την προστασία που παρέχεται από το κτήριο και μέσω κατάλληλων μέτρων που περιλαμβάνουν:
  - ○ Ερμάρια αρχειοθέτησης τα οποία κλειδώνονται με κλειδιά που βρίσκονται μακριά από τα ντουλάπια,
  - ○ Κλειδωμένα χρηματοκιβώτια,
  - ○ Αποθήκευση σε Ασφαλή Περιοχή με έλεγχο πρόσβασης.
- ✓ Για την απόρριψη άχρηστων / αποσυρόμενων εγγράφων χρησιμοποιείται κάδος ανακύκλωσης του δήμου αφού έχει προηγηθεί καταστροφή με τεμαχιστικό μηχάνημα (shredder) κάθε εγγράφου που απορρίπτεται,
- ✓ Οι επιφάνειες των γραφείων και των λοιπών επίπλων των θέσεων εργασίας του προσωπικού διατηρούνται απολύτως ελεύθερες από οποιοδήποτε έγγραφο όταν δεν χρησιμοποιούνται από τον εξουσιοδοτημένο υπάλληλο για κάθε θέση εργασίας (clean desk),
- ✓ Οι οθόνες των ηλεκτρονικών υπολογιστών των θέσεων εργασίας του προσωπικού απενεργοποιούνται εντός max 3 min όταν δεν χρησιμοποιούνται (screen saver setting : 3 min με αίτημα εισαγωγής username / password),
- ✓ Όλος ο γενικός εξοπλισμός υπολογιστών βρίσκεται σε κατάλληλες θέσεις / χώρους που παρέχουν προστασία από:
  - ○ περιβαλλοντικούς κινδύνους (π.χ. ζέστη, φωτιά, καπνό, νερό και σκόνη),
  - ○ κίνδυνο κλοπής,
  - ○ κίνδυνο από την οπτική επαφή ή την πρόσβαση από μη εξουσιοδοτημένα άτομα,

- ✓ Όλες οι πληροφορίες αποθηκεύονται σε φακέλους στον server του δικτύου όπως έχει σχεδιαστεί ώστε να είναι εύκολη η ανάκτηση τους σε περίπτωση απώλειας από βλάβη, σφάλμα δυσλειτουργία ή αστοχία κ.λ.π. μέσω της διαδικασίας του back up,
- ✓ Τεκμηρίωση της αρχιτεκτονικής και όλων των μερών του δικτύου και των στοιχείων εξοπλισμού που απαρτίζουν το σύστημα πληροφορικής και αποθήκευσή της τεκμηρίωσης με ρυθμίσεις διαμόρφωσης όλων των μερών υλικού και λογισμικού που απαρτίζουν το δίκτυο (κατάλογος που ανανεώνεται όταν προστίθενται ή αφαιρούνται περιουσιακά στοιχεία),
- ✓ Το σύστημα πληροφορικής προστατεύεται από UPS για τη μείωση του κινδύνου βλάβης ή απώλειας πληροφοριών από διαταραχές τάσης τροφοδοσίας του δικτύου ηλεκτροδότησης,
- ✓ Καλώδια που μεταφέρουν δεδομένα ή υποστηρίζουν σημαντικές υπηρεσίες πληροφοριών προστατεύονται από υποκλοπές ή ζημίες,
- ✓ Τα καλώδια ρεύματος διαχωρίζονται κατά την όδευσης τους από τα καλώδια δικτύου για την αποφυγή παρεμβολών,
- ✓ Τα καλώδια δικτύου προστατεύονται από κανάλι όδευσης και αποφεύγονται οι διαδρομές μέσω περιοχών όπου υπάρχει ελεύθερη πρόσβαση.

12. Διαχείριση Κύκλου Ζωής Εξοπλισμού (Equipment Lifecycle Management)

Γενικά Σημεία

- Η Διοίκηση της **T.B.S. s.a.** σε συνεργασία με τον Υπ. Μηχανογράφησης και τους προμηθευτές εξοπλισμού διασφαλίζουν ότι όλος ο εξοπλισμός της εταιρείας διατηρείται σύμφωνα με τις οδηγίες του κατασκευαστή και με οποιεσδήποτε εσωτερικές διαδικασίες ώστε να εξασφαλισθεί ότι παραμένει σε άριστη κατάσταση.

Ενέργειες για την συμμόρφωση

- ✓ Τήρηση αρχείου με το ιστορικό του εξοπλισμού έτσι ώστε όταν ο εξοπλισμός παλιώνει να μπορούν να παρθούν αποφάσεις σχετικά με τον κατάλληλο χρόνο που πρέπει να αντικατασταθεί. Με ευθύνη του Υπ. Μηχανογράφησης εξασφαλίζεται ότι:
  - Προσδιορίζονται οι απαιτήσεις παροχής εγγύησης καλής λειτουργίας και τεχνικής υποστήριξης κατά τις συμφωνίες προμήθειας εξοπλισμού και λογισμικού,
  - Προσδιορίζεται η συχνότητα ελέγχων / συντήρησης, περιγράφονται οι απαραίτητες σχετικές εργασίες και υλοποιούνται με συνέπεια,
  - Τηρείται αντίγραφο των οδηγιών των κατασκευαστών κάθε εξοπλισμού (διαθέσιμο στο προσωπικό υποστήριξης για χρήση όταν προγραμματίζονται και εκτελούνται επιδιορθώσεις),
  - Τηρείται λεπτομερές αρχείο των ενεργειών ελέγχου / συντήρησης / αποκατάστασης και καταγραφή λεπτομερειών σφαλμάτων διακοπής και απαιτούμενων / υλοποιούμενων ενεργειών,
  - Εφαρμόζεται κατάλληλη διαδικασία call out σε περίπτωση βλάβης, αστοχίας, δυσλειτουργίας βάσει της οποίας μόνο εξουσιοδοτημένοι τεχνικοί εκτελούν εργασίες σχετικές με το σύστημα πληροφορικής,
  - Υπάρχει πλήρης και επαρκή αδειοδότηση για το λογισμικό που εγκαθίσταται σε εξοπλισμό του συστήματος πληροφορικής της εταιρείας,

- ✓ Η χρήση του εξοπλισμού του συστήματος πληροφορικής της εταιρείας εκτός χώρων της εταιρείας απαγορεύεται χωρίς την έγκριση του Γενικού Δ/ντη,
- ✓ Διαγραφή κατά τρόπο μη αντιστρέψιμο κάθε πληροφορίας από τα ηλεκτρονικά μέσα αποθήκευσης που μεταφέρονται εκτός εταιρείας (π.χ. επιστροφή μετά από συμφωνία leasing, για επισκευή) και τήρηση αρχείου από όπου προκύπτουν η ημερομηνία και ώρα αποστολής / παραλαβής, οι υπεύθυνοι αποστολής / παραλαβής, ο προορισμός και η αιτία της μεταφοράς. Αν αυτό δεν είναι εφικτό τα αποθηκευτικά μέσα δεν μεταφέρονται εκτός εταιρείας για επισκευή και αντικαθίστανται με άλλα αφού καταστραφούν με μηχανικό τρόπο (τρυπάνι) και τηρηθεί πρωτόκολλο καταστροφής.

13. Πρόσβαση στο σύστημα πληροφορικής

Γενικά Σημεία

- Η Διοίκηση της **T.B.S. s.a.** σε συνεργασία με τον Υπ. Μηχανογράφησης εξασφαλίζει ότι η πρόσβαση στο σύστημα πληροφορικής επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες.

Ενέργειες για την συμμόρφωση

- ✓ Για την εύρυθμη και ασφαλή λειτουργία εκδίδονται και εφαρμόζονται διαδικασίες / οδηγίες τυποποιημένης λειτουργίας για τον έλεγχο πρόσβασης χρηστών οι οποίες καλύπτουν όλα τα στάδια της δραστηριότητας των χρηστών, από την αρχική εγγραφή νέων χρηστών ως την τελική διαγραφή χρηστών που δεν απαιτείται πλέον να έχουν πρόσβαση και εξασφαλίζουν τα εξής:
  - Αυθεντικοποίηση μεμονωμένων χρηστών (όχι ομάδες χρηστών, όχι γενικοί λογαριασμοί),
  - Προστασία σε ότι αφορά την ανάκτηση των κωδικών και λεπτομέρειες ασφάλειας,
  - Παρακολούθηση συστημάτων πρόσβασης και καταγραφή – σε επίπεδο χρήστη,
  - Διαχείριση ρόλων έτσι ώστε οι λειτουργίες να εκτελούνται χωρίς κοινή χρήση κωδικών.
- ✓ Λογαριασμοί και δικαιώματα «διαχειριστή συστήματος» (administrator) παρέχονται μόνο στον Υπ. Μηχανογράφησης και στον Γενικό Δ/ντη,
- ✓ Κάθε χρήστης έχει πρόσβαση και δικαιώματα για την χρήση του συστήματος πληροφορικής:
  - ανάλογα με τις εργασίες που εκτελούν,
  - μέσω μοναδικού ονόματος χρήστη (username) το οποίο:
    - δεν μοιράζεται με άλλους χρήστες,
    - δεν δίνεται ή δεν έχει δοθεί στο παρελθόν σε άλλο χρήστη,
  - μέσω μοναδικού συνθηματικού εισόδου (password) το οποίο:
    - γνωρίζει μόνο ο ίδιος,
    - αποτελείται τουλάχιστον από 8 χαρακτήρες και συμπεριλαμβάνεται σ’ αυτούς ένα ψηφίο τουλάχιστον και ένα σύμβολο,
    - ζητείται από το σύστημα να εισάγεται σε κάθε είσοδο,
    - ζητείται από το σύστημα ο χρήστης να το αλλάζει μετά από 30 ημέρες
    - δίνεται η δυνατότητα να το αλλάζει κατά την κρίση του ο κάθε χρήστης όποτε υπάρχει υπόνοια ή βεβαιότητα ότι έχει διαρρεύσει σε κάποιον άλλο,
    - είναι αδύνατο να παρακαμφθεί (με την απόκρυψη ή απομάκρυνση των ρυθμίσεων του από τον administrator χωρίς καταγραφή της παράκαμψης και απαίτηση του συστήματος για ορισμό νέου password από τον χρήστη μετά από τυχόν παράκαμψη).

- μέσω διαδικασίας εισόδου που προβλέπει τα εξής:
  - αρχική οθόνη log-in που καθιστά προφανές ότι επιτρέπονται μόνο εξουσιοδοτημένοι χρήστες,
  - μη εμφάνιση προηγούμενων πληροφοριών εισόδου π.χ. όνομα χρήστη,
  - απόκρυψη με σύμβολα των χαρακτήρων του συνθηματικού εισόδου κατά την πληκτρολόγηση,
  - κλείδωμα του λογαριασμού μετά από 2 μη επιτυχημένες προσπάθειες,

✓ Με ευθύνη του Γενικού Δ/ντη και του Υπ. Μηχανογράφησης τα δικαιώματα πρόσβασης στα υπολογιστικά συστήματα της εταιρίας:

- εκχωρούνται και τροποποιούνται μετά από αίτημα του χρήστη στο Γενικό Δ/ντη και έγγραφη έγκριση του μετά από συνεννόηση με τον από τον υπεύθυνο του τμήματος υπό την εποπτεία του οποίου εργάζεται ο χρήστης,
- επανεξετάζονται σε τακτικά χρονικά διαστήματα (κατ'ελάχιστον κάθε 6 μήνες) για τη διασφάλιση ότι αντιστοιχούν πάντα σε κατάλληλα εξουσιοδοτημένους χρήστες και ότι είναι ανάλογα με τις εργασίες που αυτοί εκτελούν,
- διακόπτονται αμέσως όταν τερματίζεται η συνεργασία της εταιρείας με ένα εργαζόμενο ή εξωτερικό συνεργάτη (πριν την λήξη της τελευταίας ημέρας εργασίας του / συνεργασίας του με την εταιρεία).

14. Λογισμικό

Γενικά Σημεία

- Ανά πάσα στιγμή υπάρχει πλήρης και επαρκή αδειοδότηση για το λογισμικό που εγκαθίσταται σε εξοπλισμό του συστήματος πληροφορικής της εταιρείας **T.B.S. s.a.**. Η Διοίκηση εξασφαλίζει ότι επεξεργασία πληροφοριών γίνεται μόνο σε λογισμικό που είναι εγκατεστημένο σε εξοπλισμό του συστήματος πληροφορικής της εταιρείας.

Συμμόρφωση

✓ Απαγορεύεται να γίνεται επεξεργασία πληροφοριών που σχετίζεται με την δραστηριότητα της εταιρείας σε λογισμικό που δεν είναι εγκατεστημένο σε εξοπλισμό του συστήματος πληροφορικής της εταιρείας,

✓ Η προμήθεια λογισμικού που εγκαθίσταται σε εξοπλισμό του συστήματος πληροφορικής της εταιρείας εγκρίνεται από τον Γενικό Δ/ντη μετά από συνεννόηση με τον Υπ. Μηχανογράφησης,

✓ Το λογισμικό που εγκαθίσταται σε εξοπλισμό του συστήματος πληροφορικής της εταιρείας εγγράφεται στο όνομα της **T.B.S. s.a.** και το τμήμα για το οποίο θα χρησιμοποιηθεί (σε καμία περίπτωση στο όνομα μεμονωμένου χρήστη ώστε να μη δημιουργούνται προβλήματα και κίνδυνοι για την ασφάλεια πληροφοριών σε περίπτωση διακοπής της συνεργασίας της εταιρείας με τον χρήστη),

✓ Με ευθύνη του Υπ. Μηχανογράφησης συντάσσεται και τηρείται συνεχώς ενημερωμένος κατάλογος όλου του λογισμικού που έχει εγκατασταθεί σε εξοπλισμό του συστήματος πληροφορικής της εταιρείας, που περιλαμβάνει:

- λογισμικό που μπορεί να έχει γίνει «download» και/ή αγοραστεί από το διαδίκτυο, Shareware, Freeware και Public Domain Software,

- ο τον τίτλο και τον εκδότη του λογισμικού,
- ο Το serial number του προϊόντος λογισμικού,
- ο Την ημερομηνία και την πηγή της απόκτησης του λογισμικού,
- ο Το σημείο του συστήματος πληροφορική όπου έχει εγκατασταθεί με αναφορά στο serial number του υλικού στο οποίο έχει εγκατασταθεί κάθε αντίγραφο,
- ο Την ύπαρξη και τοποθεσία των αντιγράφων ασφαλείας,
- ο Λεπτομέρειες και διάρκεια των διακανονισμών υποστήριξης για αναβαθμίσεις λογισμικού.

✓ Λογισμικό σε Τοπικά Δίκτυα ή σε πολλαπλές μηχανές χρησιμοποιείται μόνο σύμφωνα με τη χορηγηθείσα άδεια,

✓ Λογισμικό σε εξοπλισμό του συστήματος πληροφορικής της εταιρείας εγκαθίσταται / παραμετροποιείται / ρυθμίζεται / τροποποιείται / αναβαθμίζεται **μόνο με ευθύνη ή μετά από έγκριση του Υπ. Μηχανογράφησης** μόλις ολοκληρωθούν οι απαιτήσεις εγγραφής,
Απαγορεύεται να εγκαθίσταται προσωπικό ή ανεπιθύμητο λογισμικό (π.χ. παιχνίδια, ταπετσαρίες κτλ) σε εξοπλισμό του συστήματος πληροφορικής της εταιρείας **(αποτελεί ενέργεια υψηλού κινδύνου για την ασφάλεια πληροφοριών),**

✓ Το σύστημα πληροφορικής της εταιρείας διαθέτει μηχανισμό ελέγχου και παρακολούθησης των αλλαγών στο λογισμικό που είναι εγκατεστημένο στα στοιχεία του συστήματος. Ο Υπ. Μηχανογράφησης αναφέρει **άμεσα** στον Γενικό Δ/ντη περιπτώσεις εντοπισμού μη εξουσιοδοτημένων αλλαγών οι οποίες στα πλαίσια του συστήματος διαχείρισης αντιμετωπίζονται ως περιστατικά παραβίασης της ασφάλειας των πληροφοριών.