Πολιτική Ασφάλειας Πληροφοριών

Συντάκτης Εγγράφου: **Δ/νουσα Σύμβουλος ΝΝΤ**

Έγκριση Εγγράφου: **Πρόεδρος ΔΣ ΝΝΤ**

Περιεχόμενα

1. Αρχές Ασφάλειας Πληροφοριών

Αρχές Ασφάλειας Πληροφοριών:-

- Οι πληροφορίες είναι περιουσιακό στοιχείο. Όπως κάθε άλλο επιχειρησιακό περιουσιακό στοιχείο έχει αξία και πρέπει να προστατεύεται.
- Τα συστήματα που μας επιτρέπουν να αποθηκεύουμε, επεξεργαζόμαστε και να διαμοιράζουμε πληροφορίες πρέπει επίσης να προστατεύονται.
- Τα 'Πληροφοριακά Συστήματα' είναι ο συλλογικός όρος για τις πληροφορίες και για τα συστήματα που χρησιμοποιούμε για την αποθήκευση, επεξεργασία και τον διαμοιρασμό.
- Η πρακτική της ασφάλειας των πληροφοριακών συστημάτων είναι γνωστή ως "Ασφάλεια πληροφοριών".

Η **ΝΝΤ** έχει εφαρμόσει ένα 'Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών' με σκοπό να διαχειρίζεται και συνεχώς να βελτιώνει την Ασφάλεια Πληροφοριών με το χρόνο.

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

Η Διοίκηση της ΝΝΤ δηλώνει επίσης 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 ΝΝΤ 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 Διοίκηση της ΝΝΤ θεωρεί την παρούσα Πολιτική Ασφάλειας των Πληροφοριών δεσμευτική για όλο το προσωπικό και τους συνεργάτες της εταιρείας των οποίων η δραστηριότητα μπορεί να επηρεάσει την επίδοση της ΝΝΤ σχετικά με την Ασφάλεια των Πληροφοριών.

Η Διοίκηση της ΝΝΤ εξασφαλίζει ότι κάθε μέλος του προσωπικού της ΝΝΤ και οι εξωτερικοί συνεργάτες λαμβάνουν γνώση και δεσμεύονται να τηρούν την εν λόγω Πολιτική.

Αυτό το έγγραφο πρέπει να διαβαστεί σε συνδυασμό με τις Περιγραφές Θέσης Εργασίας και τις Διαδικασίες και τις Οδηγίες της **ΝΝΤ** που καθορίζουν τις αρμοδιότητες ασφάλειας πληροφοριών όλων των χρηστών των συστημάτων ΙΤ και του εξοπλισμού μέσα στην **ΝΝΤ.**

Γενικές Αρχές

Γενικά Σημεία

- Η Ασφάλεια των Πληροφοριών είναι αρμοδιότητα όλων.
- Τα πληροφοριακά συστήματα της **NNT** παρέχονται μόνο για χρήση μέσα στην επιχείρηση.
- Χρήση οποιουδήποτε πληροφοριακού συστήματος της **NNT** για προσωπικούς λόγου (συμπεριλαμβανομένων e-mail και του δικτύου) επιτρέπεται μόνο σύμφωνα με τις οδηγίες αυτής της πολιτικής.
- η **NNT** διατηρεί το δικαίωμα να παρακολουθεί κάθε πλευρά των πληροφορικών συστημάτων του με σκοπό να προστατέψει τα νόμιμα επιχειρησιακά του δικαιώματα. Οι πληροφορίες που συλλέγονται από κάθε παρακολούθηση μπορεί να χρησιμοποιηθούν για να κινήσουν ή να υποστηρίξουν πειθαρχικές διαδικασίες.
- Δεν πρέπει να υπάρχουν προσδοκίες ιδιωτικότητας όταν χρησιμοποιούνται τα πληροφοριακά συστήματα της **NNT**.
- Παραβίαση της πολιτικής αυτής θα έχει ως αποτέλεσμα πειθαρχικές ενέργειες. Ανάλογα με την σοβαρότητα της παραβίασης, αυτές μπορεί να συμπεριλαμβάνουν:-
  - Ανεπίσημη προειδοποίηση από έναν υπεύθυνο
  - Επίσημη γραπτή ή προφορική προειδοποίηση για σοβαρό παράπτωμα
  - Απόλυση λόγω σοβαρού παραπτώματος
  - Ποινικές διαδικασίες
  - Αστικές διαδικασίες για την αποκατάσταση των ζημιών
- Αυτή η πολιτική αναφέρεται σε πολλά μέρη για πράγματα τα οποία “Άλλοι μπορεί να τα βρουν προσβλητικά”. Αυτά συμπεριλαμβάνουν αλλά δεν περιορίζονται σε: -
  - Πορνογραφικό ή σεξουαλικό υλικό
  - Ρατσιστικό, σεξιστικό ή ομοφοβικό υλικό
  - Άγευστο υλικό (όπως απεικόνιση τραυματισμού ή βασανισμός ζώων)

Συμμόρφωση

- ✓ Να είστε προσεκτικοί και να χρησιμοποιείτε λογική στη χρήση των πληροφοριακών συστημάτων.
- ✓ Αναφέρετε κάθε περιστατικό σχετικό με την ασφάλεια στον Διευθύνοντα Σύμβουλο .
- ✓ Ανατρέξτε στο γλωσσάρι στο πίσω μέρος αν χρειαστείτε κάποιον ορισμό κάποιου όρου αυτού του εγγράφου.

2. Διαχείριση Επικοινωνιών και Λειτουργιών - Communications and Operations Management

Λειτουργικές Διαδικασίες και Αρμοδιότητες

Γενικά Σημεία

- Οι λειτουργικές διαδικασίες χρησιμοποιούνται για την καθημερινή συντήρηση των IT συστημάτων και υποδομής της **NNT** με σκοπό να διασφαλίσουν την υψηλότερη πιθανή υπηρεσία από αυτά τα περιουσιακά στοιχεία
- Αλλαγές στα λειτουργικά συστήματα του οργανισμού ελέγχονται με μία επίσημη διαδικασία ελέγχου αλλαγής.
- Τα αναπτυξιακά και δοκιμαστικά περιβάλλοντα πρέπει να είναι ξεχωριστά από το ζωντανό λειτουργικό περιβάλλον για τη μείωση κινδύνου τυχαίων αλλαγών ή μη εξουσιοδοτημένης πρόσβασης.

Συμμόρφωση

- ✓ Καταγραφή λειτουργικών διαδικασιών σε κατάλληλο επίπεδο λεπτομερειών για την ομάδα του τμήματος που θα τα χρησιμοποιήσει.
- ✓ Αξιολόγηση όλων των σημαντικών αλλαγών στην κύρια υποδομή (π.χ. δίκτυο, κατάλογοι) για την επίπτωσή τους στην ασφάλεια πληροφοριών ως κομμάτι της τυπικής αξιολόγησης κινδύνου.
- ✓ Διαχωρισμός του περιβάλλοντος ανάπτυξης και ελέγχου από τους πιο κατάλληλους ελέγχους, συμπεριλαμβανομένων των ακόλουθων:
    - Εκτέλεση σε ξεχωριστούς υπολογιστές, domains και δίκτυα.
    - Διαφορετικά usernames και κωδικοί.
    - Καθήκοντα σε αυτούς που είναι ικανοί να αξιολογήσουν και να δοκιμάσουν λειτουργικά συστήματα.

Σχεδιασμός Συστήματος και αποδοχή - System Planning and Acceptance

Γενικά Σημεία

- Όλα τα συστατικά ή δυνατότητες της υποδομής ΙΤ της **ΝΝΤ** καλύπτονται από το σχέδιο ικανότητας πόρων και τις στρατηγικές αντικατάστασης για τη διασφάλιση ότι η αυξανόμενη δύναμη και οι απαιτήσεις αποθήκευσης δεδομένων μπορούν να δρομολογηθούν και να εκπληρωθούν εγκαίρως.

- Σημαντικά συστατικά ΙΤ περιλαμβάνουν, αλλά δεν είναι υποχρεωτικά, τα παρακάτω:

    - File servers.
    - Domain servers.
    - E-mail servers.
    - Web servers.
    - Εκτυπωτές.
    - Δίκτυα.
    - Περιβαλλοντικοί έλεγχοι συμπεριλαμβανομένου του κλιματισμού.

Συμμόρφωση

- ✓ Όλα τα τμήματα πρέπει να ενημερώνουν τον **Διευθύνοντα Σύμβουλο** για όλες τις απαιτήσεις νέων προϊόντων ή κάθε αναβάθμισης, ή βελτιώσεις που απαιτούνται για τα υπάρχοντα συστήματα.
- ✓ Όλα τα νέα προϊόντα πρέπει αγοράζονται μέσω του **Διευθύνοντος Σύμβουλου.**
- ✓ Νέα πληροφοριακά συστήματα, αναβαθμίσεις υπηρεσιών, patches και αλλαγές πρέπει να υποβάλλονται όλα στον κατάλληλο έλεγχο πριν την αποδοχή και εφαρμογή τους στο ζωντανό περιβάλλον.
- ✓ Τα κριτήρια αποδοχής πρέπει να προσδιορίζονται και να συμφωνούνται σαφώς και να καταγράφονται και πρέπει να περιλαμβάνουν διαχείριση εξουσιοδότησης.
- ✓ Εφαρμογές τρίτων μερών πρέπει επίσης να παρακολουθούνται για service packs και patches.
- ✓ Σημαντικές αναβαθμίσεις του συστήματος πρέπει να ελέγχονται διεξοδικά παράλληλα με το υπάρχον σύστημα σε ένα ασφαλές περιβάλλον δοκιμών που δημιουργεί διπλότυπο του λειτουργικού συστήματος.

Προστασία ενάντια σε Κακόβουλο και Mobile Κώδικα - Protection against Malicious and Mobile Code

Γενικά Σημεία

- Πρέπει να γίνονται τα κατάλληλα βήματα για την προστασία των IT συστημάτων, της υποδομής και των πληροφοριών της **NNT** εναντίων κακόβουλου κώδικα.
- Ενεργοποίηση αποδοτικού και ενημερωμένου λογισμικού προστασίας από ιούς σε όλους τους servers και υπολογιστές.
- Με σκοπό την αποτροπή του κακόβουλου κώδικα, πρέπει να διεξάγονται κατάλληλοι έλεγχοι πρόσβασης (πχ. Δικαιώματα διαχειριστή, χρήστη) για την αποτροπή εγκατάστασης λογισμικού από όλους τους χρήστες.
- Ο κινητός κώδικας παρουσιάζεται σε νέες τεχνολογίες οι οποίες συχνά βρίσκονται στις ιστοσελίδες, στα emails, και περιλαμβάνονται, αλλά όχι μόνο σε:
    - ActiveX.
    - Java.
    - JavaScript.
    - VBScript.
    - Macros.
    - HTTPS.
    - HTML.

Συμμόρφωση

- ✓ Το προσωπικό της **NNT** είναι υπεύθυνο για τη διασφάλιση ότι δεν εισάγεται κακόβουλος κώδικας στα IT συστήματα της **NNT**.
- ✓ Όποιος εντοπίζει ιό σε κάποιο σύστημα της **NNT** πρέπει να ενημερώσει τον Δ/ντα Σύμβουλο.
- ✓ Όλοι οι servers πρέπει να έχουν κριτήρια ασφάλειας των patches που θα εφαρμοστούν με του που γίνουν διαθέσιμα και θα έχουν περάσει τον έλεγχο αποδοχής συστήματος. Όλα τα υπόλοιπα patches πρέπει να εφαρμοστούν κατάλληλα.
- ✓ Patches πρέπει να εφαρμόζονται κατάλληλα σε όλα τα λογισμικά του δικτύου του οργανισμού.
- ✓ Πρέπει 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.
- ✓ Αντι-ικό λογισμικό θα εγκαθίσταται σε κατάλληλα σημεία του δικτύου και στους επισκέπτες.

Αντίγραφα Ασφαλείας – Backups

Γενικά Σημεία

- Πρέπει να λαμβάνονται τακτικά αντίγραφα ασφαλείας των ευαίσθητων πληροφοριών της επιχείρησης για τη διασφάλιση ότι ο οργανισμός μπορεί να ανακάμψει από κάποια καταστροφή, αποτυχία μέσου ή σφάλμα.
- Ένας κατάλληλος κύκλος αντιγράφων ασφαλείας πρέπει να χρησιμοποιείται και να τεκμηριώνεται πλήρως
- Οποιοδήποτε 3ο μέρος αποθηκεύει επιχειρησιακές πληροφορίες πρέπει επίσης να απαιτείται να διασφαλίσει ότι οι πληροφορίες αποθηκεύονται σε αντίγραφα ασφαλείας.

Συμμόρφωση

- ✓ Αποθήκευση όλης της έγγραφης τεκμηρίωσης των αντιγράφων ασφαλείας, συμπεριλαμβανομένης μίας ολοκληρωμένης εγγραφής του τι έχει αποθηκευτεί σε αντίγραφο ασφαλείας μαζί με τη διαδικασία ανάκαμψης, σε μία τοποθεσία εκτός του χώρου με επιπλέον αντίγραφο στον κύριο χώρο.
- ✓ Αυτά θα συνοδεύονται από ένα κατάλληλο σύνολο αποθηκευτικών μέσων που θα φυλλάσσονται σε ασφαλή περιοχή.
- ✓ Διασφάλιση ότι η απομακρυσμένη τοποθεσία είναι αρκετά μακριά ώστε να αποφευχθεί η επίδρασή του από όποια καταστροφή προκύψει στο κύριο χώρο.
- ✓ Πρέπει να δημιουργείται και να αποθηκεύεται πλήρη; τεκμηρίωση της διαδικασίας ανάκαμψης
- ✓ Εκτέλεση τακτικών ανακτήσεων αποθηκευμένων πληροφοριών σε μέσα αντιγράφων ασφαλείας για τη διασφάλιση της αξιοπιστίας των μέσων και της διαδικασίας αποθήκευσης.

Χειρισμός Μέσων Αποθήκευσης - Storage Media Handling

Γενικά Σημεία

- Επιτρεπτά μέσα αποθήκευσης στην NNT είναι :
    - Σκληροί δίσκοι υπολογιστών (εσωτερικοί και εξωτερικοί)
    - CD
    - DVD
    - Οπτικοί δίσκοι - Optical Disks
    - Ψηφιακές Κάμερες

- Τα αφαιρούμενα μέσα υπολογιστών (πχ. δίσκοι) πρέπει να προστατεύονται για να αποφευχθεί η ζημιά, κλοπή ή μη εξουσιοδοτημένη πρόσβαση.
- Τα μέσα αποθήκευσης που μεταφέρονται πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, λανθασμένη χρήση ή διακοπή.
- Η τεκμηρίωση του συστήματος πρέπει να προστατεύεται από μη εξουσιοδοτημένη πρόσβαση. Αυτό συμπεριλαμβάνει κατά παραγγελία τεκμηρίωση που έχει δημιουργηθεί από τον **Διευθύνοντα Σύμβουλο** ή όποιο άλλο προσωπικό (αυτά δεν περιλαμβάνουν γενικά εγχειρίδια που έχουν προμηθευτεί με λογισμικό)
- Παραδείγματα των εγγράφων που πρέπει να προστατευτούν συμπεριλαμβάνουν, αλλά δεν περιορίζονται, περιγραφές από:
    - Εφαρμογές
    - Διαδικασίες
    - Διεργασίες
    - Δομές Δεδομένων
    - Λεπτομέρειες εξουσιοδότησης

Συμμόρφωση

- ✓ Διατήρηση εγγράφων διαδικασιών για δημιουργία εφεδρικών αντιγράφων ασφαλείας εκτός επιχείρησης
- ✓ Διατήρηση των μέσων αποθήκευσης σε ασφαλές περιβάλλον
- ✓ Όπου απαιτούνται courier, πρέπει να δημιουργηθεί μία λίστα με τις αξιόπιστες courier
- ✓ Διασφάλιση ότι τα μέσα αποθήκευσης που δεν απαιτούνται πλέον απορρίπτονται με ασφάλεια και σιγουριά για την αποφυγή διαρροής δεδομένων
- ✓ Θα πρέπει να εφαρμόζεται αποτελεσματικός έλεγχος σε όλα τα έγγραφα και την αποθήκευση των εγγράφων.

Παρακολούθηση - Monitoring

Γενικά Σημεία

- Είναι δυνατό για την επίτευξη της ασφάλειας και για την διευκόλυνση της διερεύνησης περιστατικών να εφαρμόζονται τεχνικές παρακολούθησης. Στην περίπτωση αυτή τα αρχεία καταγραφής ελέγχου (audit logs) πρέπει να περιέχουν κατ' ελάχιστο τις ακόλουθες πληροφορίες:

    - Ταυτότητα συστήματος (System identity).
    - Όνομα χρήστη.
    - Επιτυχής/Ανεπιτυχής είσοδος.
    - Επιτυχής/Ανεπιτυχής έξοδος.
    - Μη εξουσιοδοτημένη πρόσβαση.
    - Αλλαγές στις ρυθμίσεις του συστήματος system configurations).
    - Χρήση προνομιακών λογαριασμών (π.χ. διαχείριση λογαριασμών, αλλαγές στην πολιτική).

Συμμόρφωση

- ✓ Διατήρηση αρχείων καταγραφής ελέγχου για τουλάχιστον 6 μήνες που θα καταγράφουν τις εξαιρέσεις και άλλα περιστατικά σχετικά με την ασφάλεια.
- ✓ Προστασία πρόσβασης στις εγγραφές από μη εξουσιοδοτημένη πρόσβαση που θα έχει ως αποτέλεσμα την αλλαγή ή διαγραφή καταχωρημένων πληροφοριών
- ✓ Πρόληψη των διαχειριστών του συστήματος από τη διαγραφή ή απενεργοποίηση καταχωρήσεων από δικιά τους δραστηριότητα
- ✓ Λειτουργικό προσωπικό και διαχειριστές συστήματος πρέπει να διατηρούν αρχείο των δραστηριοτήτων τους
- ✓ Τα αρχεία μπορεί να περιλαμβάνουν:

    - Back-up timings and details of exchange of backup tapes.
    - System event start and finish times and who was involved.
    - System errors (what, date, time) and corrective action taken.

- ✓ Τα αρχεία πρέπει να ελέγχονται τακτικά για να διασφαλιστεί ότι ακολουθούνται οι κατάλληλες διαδικασίες.
- ✓ Όλα τα ρολόγια των υπολογιστών πρέπει να συγχρονιστούν με την προέλευση της ώρας GSI για να διασφαλιστεί η ακρίβεια όλων των αρχείων καταγραφής ελέγχου των συστημάτων καθώς μπορεί να χρειαστούν για διερεύνηση περιστατικών.

Διαχείριση Δικτύου - Network Management

Γενικά Σημεία

- Η διαχείριση του δικτύου είναι κρίσιμη για την παροχή υπηρεσιών οργάνωσης
- Συνδέσεις στο δίκτυο της **NNT** γίνονται με ελεγχόμενο τρόπο.
- Ασύρματα δίκτυα πρέπει να εφαρμόζουν ελέγχουν για την προστασία των δεδομένων που διακινούνται στο δίκτυο και αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Συμμόρφωση

- ✓ Διασφάλιση ότι υπάρχουν ξεκάθαρες αρμοδιότητες και διαδικασίες για τη διαχείριση του κινητού εξοπλισμού και των χρηστών
- ✓ Κατά περίπτωση, θέστε ελέγχους για την προστασία των δεδομένων που διακινούνται στο δίκτυο (π.χ. κρυπτογράφηση)
- ✓ Καταγραφή της αρχιτεκτονικής του δικτύου και αποθήκευσή της με ρυθμίσεις διαμόρφωσης όλων των μερών υλικού και λογισμικού που απαρτίζουν το δίκτυο
- ✓ Καταγραφή όλων των μερών του δικτύου σε μία καταχώρηση περιουσιακού στοιχείου
- ✓ Διασφάλιση ότι όλοι οι hosts έχουν ικανοποιητικό επίπεδο ασφαλείας
- ✓ Επανεξέταση 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 πρέπει να εφαρμόζεται ως το ελάχιστο

Ασφάλεια πληροφοριών στις σχέσεις με προμηθευτές / εξωτερικούς συνεργάτες – Supplier Information Security

Γενικά Σημεία

- Κατά την δραστηριοποίηση της εταιρείας είναι πιθανόν να παραστεί ανάγκη προμήθειας υπηρεσιών ή προϊόντων που μπορούν να επιδράσουν στην ασφάλεια των πληροφοριών που διαχειρίζεται η ΝΝΤ, όπως υπηρεσίες μηχανογραφικής υποστήριξης, υπηρεσίες νομικής υποστήριξης, εξοπλισμός μηχανογράφησης και τηλεπικοινωνιών, υπηρεσίες φύλαξης, ταχυδρομικές υπηρεσίες, υπηρεσίες ενοικίασης χώρων.
- Πριν από κάθε συνεργασία με προμηθευτή προϊόντων ή υπηρεσιών η ΝΝΤ προσδιορίζει τις απαιτήσεις έτσι ώστε να μετριάζεται ο κίνδυνος για την ασφάλεια των πληροφοριών από την πρόσβαση του προμηθευτή στις πληροφορίες.
- Οι απαιτήσεις αυτές συμφωνούνται με τον προμηθευτή και η ικανοποίησή τους παρακολουθείται στα πλαίσια υπογραφής συμβάσεων συνεργασίας μέσω των οποίων προσδιορίζονται:
  - οι πληροφορίες στις οποίες θα έχει πρόσβαση ο προμηθευτής και το είδος, μεθοδολογία, διάρκεια της πρόσβασης
  - η έννοια της ασφάλειας (availability, accessibility, integrity, confidentiality), οι απαιτήσεις ασφάλειας και το επίπεδο ασφάλειας που πρέπει να εξασφαλίζεται (classification)
  - Η υποχρέωση του προμηθευτή να προστατεύει τις πληροφορίες της ΝΝΤ 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 προμηθευτής 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 ΝΝΤ 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 ειδοποίησης και συνεργασίας μεταξύ ΝΝΤ και προμηθευτή σε καταστάσεις εκτάκτου ανάγκης ή αντιμετώπισης περιστατικών ασφάλειας πληροφοριών
  - Η διαδικασία χειρισμού περιπτώσεις παράδοσης εκ μέρους του προμηθευτή προϊόντος ή υπηρεσίας μη συμμορφούμενη προς τις συμφωνημένες απαιτήσεις
  - Οι απαιτήσεις για τις υποδομές και εγκαταστάσεις της ΝΝΤ που θα πρέπει α αξιοποιηθούν κατά την προμήθεια / συνεργασία καθώς και οι απαιτήσεις εκπαίδευσης, γνώσεων και εμπειρίας που πρέπει να ικανοποιεί το προσωπικό της ΝΝΤ που θα εμπλακεί στην υλοποίηση
  - Τα στοιχεία ταυτότητας του προσωπικού του προμηθευτή 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 προμηθευτή να αναθέσει υπεργολαβικά σε άλλο μέρος ένα τμήμα ή το σύνολο της προμήθειας / παροχής της υπηρεσίας
  - 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 προμηθευτή να υποβάλλει αν αυτό απαιτείται περιοδικές αναφορές σχετικά με την αποτελεσματικότητα των μέτρων

Συμμόρφωση

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

Ετήσιος Έλεγχος Κατάστασης - Annual Check

Συμμόρφωση

- ✓ Κάθε 12 μήνες διεξάγεται από Εσωτερικό Έλεγχο, έλεγχος της κατάστασης όλων των συστημάτων και υποδομών IT του οργανισμού.
- ✓ Αυτός ο έλεγχος μπορεί να 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 συνοπτική αναφορά με προτάσεις για βελτίωση.

3. Υποδομή IT - IT Infrastructure

Ασφαλείς Περιοχές - Secure Areas

Γενικά Σημεία

- Ευαίσθητες πληροφορίες **πρέπει** να αποθηκεύονται με ασφάλεια.
- Μία αξιολόγηση κινδύνου πρέπει να προσδιορίζει το **κατάλληλο** επίπεδο προστασίας που πρέπει να εφαρμοστεί για την ασφάλεια των αποθηκευμένων πληροφοριών.
- Η φυσική προστασία πρέπει να ξεκινάει με το ίδιο το κτήριο και πρέπει να διεξάγεται μία αξιολόγηση της ευπάθειας της περιμέτρου

Συμμόρφωση

- ✓ Το κτήριο πρέπει να διαθέτει **κατάλληλους** μηχανισμούς ελέγχου για τους τύπους των πληροφοριών και τον εξοπλισμό που αποθηκεύεται εκεί. Αυτοί μπορεί να περιλαμβάνουν τα ακόλουθα:
    - Οι τοποθετημένοι συναγερμοί ενεργοποιούνται εκτός των εργάσιμων ωρών
    - Κλείδωμα πορτών και παραθύρων
    - Μπάρες στα παράθυρα για τα επίπεδα στους χαμηλούς ορόφους.
    - Τοποθέτηση μηχανισμών ελέγχου πρόσβασης σε όλες τις προσβάσιμες πόρτες (όπου χρησιμοποιούνται κωδικοί, πρέπει να αλλάζουν συχνά και να είναι γνωστοί σε αυτούς που είναι εξουσιοδοτημένοι να έχουν πρόσβαση στην περιοχή ή στο κτήριο).
    - Κάμερες CCTV
    - Στελέχωση χώρου υποδοχής
    - Προστασία κατά των καταστροφών- π.χ. φωτιά, πλημμύρα, βανδαλισμό
- ✓ Οι επισκέπτες στις προστατευόμενες περιοχές απαιτείται να εγγράφονται κατά την είσοδο και έξοδο με αναφορά στην ώρα εισόδου / εξόδου
- ✓ Ένας υπάλληλος του οργανισμού πρέπει να επιτηρεί συνέχεια όλους τους επισκέπτες που έχουν πρόσβαση σε προστατευμένες περιοχές
- ✓ Τα κλειδιά όλων των προστατευόμενων περιοχών και των περιοχών που έχουν IT εξοπλισμό πρέπει να φυλάσσονται κεντρικά από τον **Διευθύνοντα Σύμβουλο**,
- ✓ Σε όλες τις περιπτώσεις όπου εφαρμόζονται οι διαδικασίες ασφάλειας, πρέπει να εκδίδονται οδηγίες για την αντιμετώπιση περιπτώσεων παραβίασης της ασφάλειας

Ασφάλεια Εγγράφων και Εξοπλισμού - Paper and Equipment Security

Γενικά Σημεία

- Για να επιτραπεί η πρόσβαση σε έγγραφες (ή μη ηλεκτρονικές) πληροφορίες πρέπει να εκχωρείται εξουσιοδότηση και οι πληροφορίες να χαρακτηρίζονται από πλευράς απαιτούμενου επίπεδου ασφάλειας (classification) ένας κάτοχος και μια ταξινόμηση.

Συμμόρφωση

- ✓ Τα έγγραφα σε ένα ανοιχτό γραφείο προστατεύονται ανάλογα με την προστασία που παρέχεται από το κτήριο και μέσω κατάλληλων μέτρων που μπορεί να περιλαμβάνουν :
  - Ντουλάπια αρχειοθέτησης τα οποία κλειδώνονται με κλειδιά που βρίσκονται μακριά από τα ντουλάπια.
  - Κλειδωμένα χρηματοκιβώτια.
  - Αποθήκευση σε Ασφαλή Περιοχή με ελέγχους πρόσβασης.
- ✓ Όλος ο γενικός εξοπλισμός υπολογιστών πρέπει να βρίσκεται σε κατάλληλες φυσικές τοποθεσίες που:
  - Εξαλείφουν τον κίνδυνο από περιβαλλοντικούς κινδύνους – π.χ. ζέστη, φωτιά, καπνό, νερό και σκόνη
  - Εξαλείφουν τον κίνδυνο κλοπής
  - Επιτρέπουν στους σταθμούς εργασίας να διαχειρίζονται ευαίσθητα δεδομένα τοποθετώντας με τέτοιο τρόπο ώστε να εξαλειφθεί ο κίνδυνος να τα δουν μη εξουσιοδοτημένα άτομα.
- ✓ Τα δεδομένα πρέπει να αποθηκεύονται στους servers του δικτύου όπου χρειάζεται. Αυτό εξασφαλίζει ότι οι πληροφορίες που θα χαθούν, κλαπούν ή καταστραφούν από μη εξουσιοδοτημένη πρόσβαση, μπορούν να αποκατασταθούν στο ακέραιο.
- ✓ Κρίσιμα επιχειρησιακά συστήματα πρέπει να προστατεύονται από ένα UPS για τη μείωση του κινδύνου των λειτουργικών συστημάτων και τη διακοπή δεδομένων, από πτώση της τάσης.
- ✓ Όλα τα στοιχεία του εξοπλισμού πρέπει να καταγράφονται σε έναν κατάλογο που ανανεώνεται όταν προστίθενται ή αφαιρούνται περιουσιακά στοιχεία.
- ✓ Καλώδια που μεταφέρουν δεδομένα ή υποστηρίζουν σημαντικές υπηρεσίες πληροφοριών πρέπει να προστατεύονται από υποκλοπές ή ζημίες.
- ✓ Τα καλώδια ρεύματος πρέπει να είναι ξεχωριστά από τα καλώδια δικτύου για την αποφυγή παρεμβολών.
- ✓ Τα καλώδια δικτύου πρέπει να προστατεύονται από τον αγωγό και όπου γίνεται να αποφεύγονται οι διαδρομές μέσω περιοχών όπου υπάρχει ελεύθερη πρόσβαση δημόσια.

Διαχείριση Κύκλου Ζωής Εξοπλισμού - Equipment Lifecycle Management

Γενικά Σημεία

- Ο **Δ/νων Σύμβουλος** και οι τυχόν εξωτερικοί συνεργάτες Μηχανογραφικής Υποστήριξης ή / και προμηθευτές πρέπει να διασφαλίσουν ότι όλος ο εξοπλισμός της **ΝΝΤ** διατηρείται σύμφωνα με τις οδηγίες του κατασκευαστή και με οποιεσδήποτε εσωτερικές διαδικασίες ώστε να εξασφαλισθεί ότι παραμένει σε άριστη κατάσταση.

Συμμόρφωση

- ✓ Το προσωπικό που εμπλέκεται με τη συντήρηση πρέπει:
  - Να διατηρεί αντίγραφα των οδηγιών των κατασκευαστών.
  - Να προσδιορίζονται τα συνιστώμενα διαστήματα ελέγχων και οι απαιτήσεις.
  - Ενεργοποίηση μιας διαδικασίας call out σε περίπτωση αποτυχίας.
  - Διασφάλιση ότι μόνο εξουσιοδοτημένοι τεχνικοί εκτελούν κάποια δουλειά στο περιβάλλον.
  - Καταγραφή λεπτομερειών όλων των ενεργειών αποκατάστασης που θα διεξαχθούν.
  - Προσδιορισμός απαιτήσεων εγγύησης.
  - Καταγραφή λεπτομερειών σφαλμάτων διακοπής και απαιτούμενων ενεργειών.
- ✓ Ένα υπηρεσιακό αρχείο ιστορικού του εξοπλισμού πρέπει να διατηρείται έτσι ώστε όταν ο εξοπλισμός παλιώνει να μπορούν να παρθούν αποφάσεις σχετικά με τον κατάλληλο χρόνο που πρέπει να αντικατασταθεί.
- ✓ Η συντήρηση του εξοπλισμού πρέπει να είναι σύμφωνη με τις οδηγίες του κατασκευαστή. Αυτή πρέπει να καταγράφεται και να είναι διαθέσιμη στο προσωπικό υποστήριξης για να τη χρησιμοποιεί όταν προγραμματίζει επιδιορθώσεις.
- ✓ Η χρήση του εξοπλισμού εκτός χώρου πρέπει να εγκρίνεται επίσημα από τον Δ/νων Σύμβουλο..
- ✓ Εξοπλισμός ο οποίος θα επαναχρησιμοποιηθεί ή θα αποσυρθεί πρέπει να έχει όλα τα δεδομένα και το λογισμικό σβησμένα/καταστρεμμένα.
- ✓ Αν ο εξοπλισμός θα περάσει σε άλλο οργανισμό (π.χ. επιστροφή μετά από συμφωνία leasing) η αφαίρεση των δεδομένων πρέπει να γίνει με τη χρήση επαγγελματικών εργαλείων αφαίρεσης.
- ✓ Λογισμικά μέσα ή υπηρεσίες πρέπει να καταστρέφονται για την αποφυγή της πιθανότητας ακατάλληλης χρήσης που θα μπορούσε να παραβιάσει τους όρους και τις προϋποθέσεις των αδειών που υπάρχουν.
- ✓ Για την επιβεβαίωση της ακρίβειας και των συνθηκών παράδοσης και για την αποφυγή παράπλευρης απώλειας ή κλοπής του αποθηκευμένου εξοπλισμού, πρέπει να εφαρμόζονται τα ακόλουθα:
  - Οι παραδόσεις του εξοπλισμού πρέπει να υπογράφονται από εξουσιοδοτημένο πρόσωπο χρησιμοποιώντας μία κατάλληλη διαδικασία ελέγχου. Αυτή η διαδικασία πρέπει να επιβεβαιώνει ότι τα παραδομένα στοιχεία ανταποκρίνονται πλήρως στα συνοδευτικά έγγραφα της παράδοσης. Παραλαβή των πραγματικών περιουσιακών στοιχείων πρέπει να καταγράφεται.
  - Μεταγενέστερη απομάκρυνση του εξοπλισμού γίνεται μέσω μιας επίσημης, διαδικασίας ελέγχου.

Πρόσβαση IT - IT Access

Γενικά

Γενικά Σημεία

- Οι κωδικοί όλων των χρηστών όλων των επιπέδων πρέπει να αλλάζουν το μέγιστο κάθε 60 ημέρες ή όταν το σύστημα υποδείξει στον χρήστη αλλαγή κωδικού

Συμμόρφωση

- ✓ Όλα τα συστήματα IT και οι διαδικασίες της **NNT** στοχεύουν στην εξασφάλιση των παρακάτω:
  - Αυθεντικοποίηση μεμονωμένων χρηστών, όχι ομάδες χρηστών – δηλ. 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.
  - Οι διαδικασίες κωδικού πρόσβασης διαχειριστή πρέπει να ελέγχονται κατάλληλα, με ασφάλεια και να αξιολογούνται.
- ✓ Επίσημες διαδικασίες ελέγχου πρόσβασης χρηστών πρέπει να υπάρχουν, εφαρμόζονται και διατηρούνται ενημερωμένες για κάθε εφαρμογή και πληροφοριακό σύστημα για να διασφαλιστεί η αποτροπή μη εξουσιοδοτημένης πρόσβασης.
- ✓ Πρέπει να καλύπτονται όλα τα στάδια της δραστηριότητας των χρηστών, από την αρχική εγγραφή των νέων χρηστών ως την τελική διαγραφή των χρηστών που δεν απαιτείται πλέον να έχουν πρόσβαση.
- ✓ Κάθε χρήστης πρέπει να έχει δικαιώματα πρόσβασης και άδειες στα συστήματα υπολογιστών και δεδομένα τα οποία:
  - Είναι ανάλογα με τις εργασίες που πρόκειται να εκτελέσουν
  - Έχουν μοναδικό όνομα χρήστη το οποίο δεν μοιράζεται ή έχει δοθεί σε άλλο χρήστη.
  - Έχουν σχετικούς μοναδικούς κωδικούς που ζητούνται σε κάθε νέα είσοδο.
- ✓ Τα δικαιώματα πρόσβασης πρέπει να επανεξετάζονται σε τακτικά χρονικά διαστήματα για τη διασφάλιση ότι υπάρχουν ακόμα τα κατάλληλα δικαιώματα.
- ✓ Λογαριασμοί διαχειριστή συστήματος πρέπει να παρέχονται στους χρήστες που απαιτείται να εκτελούν εργασίες διαχειριστή.
- ✓ Αίτημα για πρόσβαση στα υπολογιστικά συστήματα της Εταιρίας πρέπει να υποβάλλονται αρχικά στο Δ/νοντα Σύμβουλο.
- ✓ Αιτήσεις για πρόσβαση πρέπει να υποβάλλονται μόνο αν έχει προηγηθεί έγκριση από τον υπεύθυνο Τομέα / Υπηρεσίας που ανήκει ο χρήστης.
- ✓ Όταν ένας υπάλληλος αφήνει την εταιρεία, η πρόσβαση του στα συστήματα υπολογιστών και στα δεδομένα πρέπει να διακόπτεται από αμέσως μετά την τελευταία εργάσιμή του μέρα. Είναι αρμοδιότητα του Δ/νοντα Σύμβουλου να εξασφαλίσει τη διακοπή των δικαιωμάτων πρόσβασης.

Έλεγχος Πρόσβασης στο Server και σε Εφαρμογές - Server and Application Access Control

Γενικά Σημεία

- Η πρόσβαση στους servers ελέγχεται από μία ασφαλή διαδικασία εισόδου
- Όλες οι προσβάσεις στα λειτουργικά συστήματα γίνονται μέσω ενός μοναδικού username που θα καταγράφεται και θα μπορεί να εντοπιστεί ξανά σε κάθε ξεχωριστό χρήστη

Συμμόρφωση

- ✓ Η διαδικασία εισόδου πρέπει επίσης να προστατεύεται από:
  - Μη εμφάνιση προηγούμενων πληροφοριών εισόδου π.χ. όνομα χρήστη
  - Περιορισμός του αριθμού των μη επιτυχημένων προσπαθειών κλείδωμα του λογαριασμού αν απαιτείται.
  - Οι χαρακτήρες των συνθηματικών κρύβονται από σύμβολα
  - Εμφάνιση μηνύματος γενικής προειδοποίησης ότι επιτρέπονται μόνο εξουσιοδοτημένοι χρήστες
- ✓ Οι διαχειριστές του συστήματος πρέπει να έχουν ξεχωριστούς λογαριασμούς διαχειριστών οι οποίοι θα καταγράφονται και θα ελέγχονται
- ✓ Ο Δ/νων Σύμβουλος είναι υπεύθυνος για την έγκριση της εκχώρησης δικαιωμάτων πρόσβασης στις πληροφορίες εντός του συστήματος.
- ✓ Αυτή η πρόσβαση πρέπει:
  - Να διαχωρίζεται σε ξεκάθαρους προκαθορισμένους ρόλους
  - Να δίνει το κατάλληλο επίπεδο πρόσβασης που απαιτείται για το ρόλο του χρήστη
  - Να είναι αδύνατο να παρακαμφθεί (με την απόκρυψη ή απομάκρυνση των ρυθμίσεων του διαχειριστή)
  - Να καταγράφεται και να αξιολογείται

Απομακρυσμένη Πρόσβαση Προμηθευτή - Supplier Remote Access

Γενικά Σημεία

- Απομακρυσμένη πρόσβαση στα συστήματα της **NNT** επιτρέπεται μόνο σε συνεργάτες / προμηθευτές που αξιολογούνται και παρακολουθούνται αυστηρά.

Συμμόρφωση

- ✓ Οποιαδήποτε αλλαγή στις συνδέσεις του συνεργάτη / προμηθευτή πρέπει να στέλνονται αμέσως στο Δ/νοντα Σύμβουλο έτσι ώστε η πρόσβαση να ανανεώνεται ή να διακόπτεται.
- ✓ Όλες οι άδειες και οι μέθοδοι πρόσβασης πρέπει να ελέγχονται από τον ή με ευθύνη του Δ/νοντα Σύμβουλου.
- ✓ Συνεργάτες / προμηθευτές πρέπει να επικοινωνούν με το Δ/νοντα Σύμβουλο πριν συνδεθούν στο δίκτυο της NNT

Λογισμικό

Γενικά Σημεία

- Η **NNT** χρησιμοποιεί λογισμικό σε όλες τις πτυχές της επιχείρησης για την υποστήριξη των δραστηριοτήτων της.
- Σε κάθε στιγμή όλο το λογισμικό που απαιτείται να υπάρχει έχει άδεια και η Εταιρία δεν ανέχεται τη χρήση κανενός λογισμικού που δεν έχει άδεια.
- Η **NNT** έχει πλήρη κατάλογο όλου του λογισμικού που έχει αγοραστεί για τους υπολογιστές και μπορεί να εγγραφεί, υποστηρίξει, και αναβαθμίσει τέτοιο λογισμικό κατάλληλα.
- Αυτό συμπεριλαμβάνει λογισμικό που μπορεί να έχει «κατέβει» και/ή αγοραστεί από το Διαδίκτυο.
- Shareware, Freeware και Public Domain Software δεσμεύονται από τις ίδιες πολιτικές και διαδικασίες όπως όλα τα υπόλοιπα λογισμικά.

Συμμόρφωση

- ✓ Όλο το απαιτούμενο λογισμικό της **NNT** πρέπει να αγοράζεται μέσω του Δ/νοντα Σύμβουλου.
- ✓ Το λογισμικό πρέπει να εγγράφεται στο όνομα της **NNT** και το τμήμα για το οποίο θα χρησιμοποιηθεί.
- ✓ Ο **Δ/νων Σύμβουλος** διατηρεί μία καταχώρηση όλου του λογισμικού της **NNT** και διατηρεί έναν κατάλογο με τις άδειες των λογισμικών. Η καταχώρηση πρέπει να περιέχει:
  a) Τον τίτλο και τον εκδότη του λογισμικού.
  b) Την ημερομηνία και την πηγή της απόκτησης του λογισμικού.
  c) Την τοποθεσία κάθε εγκατάστασης καθώς και το serial number του υλικού στο οποίο έχει εγκατασταθεί κάθε αντίγραφο.
  d) Την ύπαρξη και τοποθεσία των αντιγράφων ασφαλείας.
  e) Το serial number του προϊόντος λογισμικού.
  f) Λεπτομέρειες και διάρκεια των διακανονισμών υποστήριξης για αναβαθμίσεις λογισμικού
- ✓ Λογισμικό σε Τοπικά Δίκτυα ή σε πολλαπλές μηχανές πρέπει να χρησιμοποιείται μόνο σύμφωνα με τη χορηγηθείσα άδεια.
- ✓ Το λογισμικό πρέπει να εγκαθίσταται μόνο με έγκριση από τον **Δ/νοντα Σύμβουλο** μόλις οι απαιτήσεις εγγραφής ολοκληρωθούν.
- ✓ Όλες οι αλλαγές στο λογισμικό πρέπει να εξουσιοδοτούνται πριν εφαρμοστεί η αλλαγή.
- ✓ Σε καμία περίπτωση δεν πρέπει να εγκαθίσταται προσωπικό ή ανεπιθύμητο λογισμικό (συμπεριλαμβανομένων παιχνίδια, ταπετσαρίες κτλ) στα μηχανήματα της **NNT** καθώς υπάρχει σοβαρός κίνδυνος εισόδου ιού.
- ✓ Λόγω των αλλαγών του προσωπικού, το λογισμικό δεν πρέπει να εγγράφεται ποτέ στο όνομα μεμονωμένου χρήστη.
- ✓ Το λογισμικό δεν πρέπει να αλλάζει από κανέναν χρήστη εκτός αν υπάρχει ξεκάθαρη επιχειρησιακή ανάγκη.
- ✓ Όποιος χρήστης της **NNT** κάνει, αποκτά ή χρησιμοποιεί μη εξουσιοδοτημένο αντίγραφο του λογισμικού θα τιμωρείται κατάλληλα ανάλογα με τις περιστάσεις. Η **NNT** δεν συγχωρεί την παράνομη χρήση λογισμικού και δεν θα το ανεχτεί.