Πολιτική Ασφάλειας Πληροφοριών
VLP HELLAS SA

Πληροφορίες Εγγράφου	
Τίτλος	Πολιτική Ασφαλείας
Κατάσταση	Πολιτική Ασφαλείας 2018/06
Έκδοση	1.1
Διαβάθμιση	Εσωτερικό
Ημερομηνία	22/10/2019
Σύνταξη	Ομάδα Έργου
Έλεγχος	

Διαχείριση Τροποποιήσεων Εγγράφου		
Έκδοση	**Ημερομηνία**	**Αιτιολογία Τροποποίησης**
1.0	2019/10/22	Πρόχειρη Έκδοση

Περιεχόμενα

1. Εισαγωγή

Η Πολιτική Ασφάλειας Πληροφοριών και Δεδομένων αποτυπώνει τη θέση της Διοίκησης αναφορικά με τη στρατηγική που ακολουθεί για την ασφάλεια των πληροφοριών της και καλύπτει όλες τις ενέργειες που πρέπει να πραγματοποιούνται ώστε να οικοδομηθεί ένα ασφαλές περιβάλλον λειτουργίας στη VLP HELLAS SA.

Η αντίληψη της Διοίκησης για την ασφάλεια των πληροφοριών και η δέσμευσή της ως προς αυτή πρέπει να γίνει κατανοητή σε όλο το προσωπικό.

Η παρούσα Πολιτική Ασφάλειας Πληροφοριών αποτελεί μια σύνοψη των βασικότερων κανόνων των επιμέρους πολιτικών ασφάλειας, οι οποίοι πρέπει να τηρούνται από όλο το προσωπικό της VLP HELLAS SA και από οποιαδήποτε οντότητα έχει πρόσβαση σε πληροφορίες ή στους πληροφοριακούς πόρους της. Ως εκ τούτου, σε αυτήν περιλαμβάνεται το σύνολο των μέτρων που εφαρμόζονται και αποβλέπουν στη σύννομη, ασφαλή, αδιάλειπτη και αποτελεσματική λειτουργία των συστημάτων της VLP HELLAS SA (εφαρμογές, στοιχεία δικτύου κ.α.).

Η Πολιτική Ασφάλειας Πληροφοριών αφορά στο ελάχιστο σύνολο απαιτήσεων ασφάλειας, το οποίο απευθύνεται από τη Διοίκηση στο προσωπικό και σε όλους τους συνεργάτες της VLP HELLAS SA. Μέσα από τις γενικές αρχές, προσδιορίζεται το γενικότερο πλαίσιο ασφάλειας και διαφαίνεται η συνειδητοποίηση της σπουδαιότητας και αναγκαιότητας της προστασίας των πληροφοριών.

Η Πολιτική Ασφάλειας Πληροφοριών και οι επιμέρους πολιτικές ασφάλειας και διαδικασίες ασφάλειας βασίζονται σε διεθνώς αναγνωρισμένα πρότυπα και πηγές:

- ISO 27001 (και ISO/IEC 27002): The Standard and the Code of Practice for Information Security Management
- ISO 27005: Information Security Risk Management
- BS 25999: British Standard for Business Continuity Management
- PCI DSS 3.2
- NIST (U.S. National Institute of Standards and Technology)
- SANS (SANS Institute)

2. Σκοπός και Χρησιμότητα της Πολιτικής Ασφάλειας

Με την παρούσα Πολιτική Ασφάλειας Πληροφοριών η Διοίκηση της VLP HELLAS SA εκφράζει ρητά τη βούλησή της για τη διασφάλιση των πληροφοριών και των πληροφοριακών πόρων που υποστηρίζουν τις δραστηριότητές της και παρέχει τις βασικές κατευθύνσεις για τη διαχείριση της ασφάλειας των πληροφοριών.

Η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και συστημάτων της, σύμφωνα με την κρισιμότητά τους, είναι ουσιαστικής σημασίας για την επίτευξη των επιχειρησιακών στόχων της VLP HELLAS SA, καθώς και της συμμόρφωσής της με το ισχύον νομοθετικό και ρυθμιστικό πλαίσιο.

Η Διοίκηση υποστηρίζει ενεργά την εφαρμογή της Πολιτικής Ασφάλειας Πληροφοριών εξασφαλίζοντας τους απαραίτητους πόρους και τα μέσα για το σκοπό αυτό, καθώς επίσης και μέσω της υποδειγματικής εφαρμογής της.

3. Πεδίο Εφαρμογής

Η παρούσα Πολιτική Ασφάλειας αφορά σε όλους τους πληροφοριακούς πόρους της VLP HELLAS SA, οι οποίοι υποστηρίζουν τη διεξαγωγή των επιχειρηματικών δραστηριοτήτων της. Κατά συνέπεια, καλύπτει το σύνολο των πληροφοριών/ δεδομένων που διακινούνται, αποθηκεύονται και γενικά επεξεργάζονται στον Οργανισμό, είτε αυτές βρίσκονται σε ηλεκτρονική είτε σε έντυπη μορφή.

Η Πολιτική Ασφάλειας απευθύνεται σε όλο το προσωπικό και στους συνεργάτες οι οποίοι αποκτούν πρόσβαση στα συστήματα, στις πληροφορίες, στις υπηρεσίες και στις εγκαταστάσεις της VLP HELLAS SA.

4. Εξαιρέσεις

Οποιαδήποτε εξαίρεση από την παρούσα Πολιτική Ασφάλειας πρέπει να εγκρίνεται από την Διοίκηση της VLP HELLAS SA, πριν από οποιαδήποτε ενέργεια.

Η παρούσα πολιτική απευθύνεται στο σύνολο του προσωπικού της VLP HELLAS SA και η εφαρμογή της και η τήρησή της είναι υποχρεωτική.

5. Αξιοποίηση της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας Πληροφοριών λαμβάνει υπόψη τις απαιτήσεις ασφάλειας της οργάνωσης, λειτουργίας και τεχνικής υποδομής των πληροφοριακών πόρων της VLP HELLAS SA. Εντούτοις, η Πολιτική Ασφάλειας είναι άμεσα εξαρτημένη από τη φύση των δραστηριοτήτων της VLP HELLAS SA, τις κατευθύνσεις της Διοίκησης και το περιβάλλον λειτουργίας του Οργανισμού. Τα παρακάτω σημεία, βοηθούν στη κατανόηση της παρούσας Πολιτικής Ασφάλειας:

- Η Πολιτική Ασφάλειας Πληροφοριών αποτελεί βασικό μέσο ανάπτυξης κουλτούρας ασφάλειας στα στελέχη και στους εργαζόμενους της KVLP HELLAS SA. Αποτελεί ένα εσωτερικό έγγραφο και πρέπει να ληφθεί μέριμνα,

ώστε όλα τα μέλη του προσωπικού και οι συνεργάτες της VLP HELLAS SA που έχουν πρόσβαση στις εταιρικές πληροφορίες και στα πληροφοριακά συστήματα, είτε ως χρήστες, είτε ως διαχειριστές, είτε ως διοικητικά στελέχη, να λάβουν γνώση της.

- Η Πολιτική Ασφάλειας δεν είναι απόλυτη, ούτε στατική. Οφείλει να λαμβάνει κάθε φορά υπόψη της τις εκάστοτε μελέτες επικινδυνότητας, και τις στρατηγικές κατευθύνσεις της VLP HELLAS SA, έτσι ώστε να προσαρμόζεται και να ανταποκρίνεται εκάστοτε στις επιχειρησιακές ανάγκες.

6. Διαχείριση Πολιτικής

Ο Υπεύθυνος Ασφάλειας είναι υπεύθυνος για το περιεχόμενο, την αναπροσαρμογή και την εφαρμογή της παρούσας Πολιτικής Ασφάλειας. Επιπλέον ορίζεται ο ρόλος του υπεύθυνου επεξεργασίας προσωπικών δεδομένων για την διαχείριση των προσωπικών δεδομένων.

7. Συμμόρφωση με την Πολιτική Ασφάλειας

Όλα τα μέλη του προσωπικού, οι συνεργάτες και ανάδοχοι της VLP HELLAS SA έχουν την υποχρέωση να συμβάλλουν ενεργά στη διατήρηση της ασφάλειας των πληροφοριακών πόρων της και να συμμορφώνονται με τους αντίστοιχους κανόνες όπως έχουν καταγραφεί στην πολιτική και στις διαδικασίες ασφάλειας.

Η παραβίαση της παρούσας πολιτικής μπορεί να έχει ως συνέπεια τη λήψη πειθαρχικών ποινών. Η σκόπιμη ή επαναλαμβανόμενη παραβίαση της πολιτικής ασφάλειας μπορεί να θεωρηθεί λόγος απόλυσης, καταγγελίας ή/και λήξης συνεργασίας.

Οι πειθαρχικές ποινές θα αποφασίζονται από την Διοίκηση της VLP HELLAS SA.

8. Γενικές Αρχές

Η Πολιτική Ασφάλειας της VLP HELLAS SA, έχει αρθρωτή δομή και αποτελείται από επιμέρους πολιτικές, οι οποίες ορίζουν τις απαιτήσεις ασφάλειας που πρέπει να ικανοποιούνται για κάθε επιμέρους κατηγορία ειδικών θεμάτων.

Για την υλοποίηση των επιμέρους πολιτικών, ορίζονται, τεκμηριώνονται, εφαρμόζονται και αναθεωρούνται συγκεκριμένες διαδικασίες ασφάλειας και οργανωτικές δομές. Οι διαδικασίες ασφάλειας ορίζουν συγκεκριμένες ενέργειες των εργαζομένων, συνεργατών και χρηστών αλλά και την αλληλουχία των ενεργειών, τους υπεύθυνους για την εκτέλεσή τους και τον τρόπο και τα μέσα τεκμηρίωσής τους.

Σε όλες τις επιμέρους πολιτικές διαφαίνεται ο σημαντικός ρόλος του Υπεύθυνου Ασφαλείας που περιγράφεται αναλυτικά στην επόμενη παράγραφο.

8.1 . Ρόλοι και Αρμοδιότητες Ασφάλειας Πληροφοριών

Η VLP HELLAS SA πρέπει να διαμορφώσει τους κατάλληλους ρόλους για την αποτελεσματική διαχείριση της ασφάλειας των πληροφοριών, των πληροφοριακών και των δικτυακών της υποδομών.

Οι ευθύνες και οι αρμοδιότητες όσον αφορά στην ασφάλεια των πληροφοριών και στη διεκπεραίωση των διαδικασιών από το προσωπικό και τους εξωτερικούς συνεργάτες πρέπει να είναι σαφώς καθορισμένες και καταγεγραμμένες.

Υιοθετείται ο ρόλος του Υπεύθυνου Ασφάλειας για την κεντρική διαχείριση και τον συντονισμό των θεμάτων ασφάλειας.

Ο Υπεύθυνος Ασφαλείας πρέπει να θέτει σε εφαρμογή μέτρα ή/και διαδικασίες σχετικά με τη χρήση, τη διακίνηση και την καταστροφή των αποθηκευτικών μέσων, ηλεκτρονικών ή εντύπων, που περιέχουν δεδομένα επικοινωνίας ή άλλες πληροφορίες που μπορεί να οδηγήσουν σε αποκάλυψη δεδομένων επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών ώστε να αποτρέπεται η αποκάλυψή τους σε μη εξουσιοδοτημένα πρόσωπα.

Σκοπός του ρόλου αυτού είναι η επίβλεψη τεχνικών και άλλων θεμάτων γύρω από την ασφάλεια πληροφοριών, η εναρμόνιση της πολιτικής ασφαλείας της VLP HELLAS SA με τα διεθνή πρότυπα και η διαχείριση περιστατικών ασφαλείας.

Οι αρμοδιότητες του Υπευθύνου Ασφαλείας πιο συγκεκριμένα είναι οι παρακάτω:

- Ανάπτυξη και ενημέρωση της πολιτικής ασφαλείας
- Διεξαγωγή ελέγχων που βεβαιώνουν την ύπαρξη επιθυμητών επιπέδων ασφαλείας στις διαφορετικές τεχνολογίες που απαρτίζουν την VLP HELLAS SA
- Διακομιστές
- Δρομολογητές
- Βάσεις Δεδομένων
- Δικτυακές Εφαρμογές (Web Applications)
- Αξιολόγηση και συμμόρφωση με τα αποτελέσματα εξωτερικών ελέγχων ασφαλείας από τρίτους.
- Διεξαγωγή ελέγχου Φυσικής Ασφαλείας στους χώρους των Κέντρων Δικτύων.
- Σχεδιασμό ασφαλούς διαδικασίας δημιουργίας αντιγράφων ασφαλείας.
- Διασφάλιση ακεραιότητας αντιγράφων ασφαλείας και αρχείων καταγραφής
- Δοκιμή ορθής λειτουργίας Σχεδίου Ανάκαμψης από Καταστροφές.
- Εκπαίδευση Χρηστών για την ασφαλέστερη χρήση προσωπικών υπολογιστών στο χώρο εργασίας.
- Εκπαίδευση Διαχειριστών σχετικά με τους νέους κινδύνους στον χώρο της ασφάλειας πληροφοριών και τεχνικών αποφυγής των κινδύνων αυτών.
- Διαχείριση Περιστατικών Ασφαλείας.

Οι αρμοδιότητες του Υπεύθυνου Επεξεργασίας Προσωπικών Δεδομένων συνοψίζεται στην προστασία όλων των Προσωπικών δεδομένων που συλλέγονται κατα την λειτουργία της επιχείρησης σύμφωνα με:

Τον Νόμο 2472/1997 για την προστασία των προσωπικών δεδομένων

Τον Νόμο 3471/2006 για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες.

Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων.

Αρχείο ευαίσθητων προσωπικών δεδομένων δεν διατηρείται από την επιχείρηση.

8.2 . Καθορισμός Ιδιοκτητών Πληροφοριών

Κάθε πληροφοριακός πόρος που διαθέτει η VLP HELLAS SA και υποστηρίζει συγκεκριμένες επιχειρηματικές λειτουργίες, ανήκει σε έναν (και σε ορισμένες περιπτώσεις περισσότερους) καθορισμένο Ιδιοκτήτη Πληροφοριών ή αλλιώς χρήστες. Ο Ιδιοκτήτης Πληροφοριών φέρει τη συνολική ευθύνη για την προστασία των πληροφοριών που έχει υπό την κατοχή του και σε περίπτωση που μεταβιβάσει κάποιες από τις πληροφορίες σε τρίτους, η συνολική ευθύνη εξακολουθεί και παραμένει σε αυτόν.

8.3 . Διαβάθμιση Πληροφοριών

Όλες οι πληροφορίες που ανήκουν στην VLP HELLAS SA πρέπει να κατηγοριοποιούνται κατάλληλα από τους αντίστοιχους Ιδιοκτήτες Πληροφοριών ανάλογα με το βαθμό κρισιμότητάς τους και το Σχήμα Διαβάθμισης Πληροφοριών. Σκοπός είναι να υλοποιηθούν οι κατάλληλοι μηχανισμοί προστασίας των πληροφοριών και η διαχείρισή τους σύμφωνα με το επίπεδο διαβάθμισης που τους έχει αποδοθεί.

Το σχήμα διαβάθμισης που ακολουθεί η VLP HELLAS SA περιγράφεται αναλυτικά στο έγγραφο «E_07 Σχήμα Διαβάθμισης Πληροφοριών».

8.4 . Διαχείριση Κινδύνων

Η VLP HELLAS SA πρέπει να διενεργεί αποτίμηση των κινδύνων της ασφάλειας πληροφοριών μια φορά το χρόνο κατά ελάχιστο. Μέσω της διαδικασίας αυτής ο οργανισμός είναι σε θέση να αναγνωρίζει και να εξετάζει τις αδυναμίες, τις πιθανές απειλές προς τους πόρους της, την πιθανότητα εκδήλωσής τους και κατά συνέπεια τον κίνδυνο που διατρέχουν. Σκοπός είναι να καθοριστούν κατάλληλες ενέργειες και οι προτεραιότητες της VLP HELLAS SA απέναντι στους κινδύνους που διατρέχει η ασφάλεια των πληροφοριών της και να οδηγήσουν σε πιθανή αναθεώρηση της ισχύουσας Πολιτικής Ασφαλείας όταν αυτό χρειάζεται.

Τα αποτελέσματα της αποτίμησης κινδύνου διατηρούνται και είναι διαθέσιμα κατά

τον τακτικό ή έκτακτο έλεγχο από τις αρμόδιες αρχές.

8.5 . Διαχείριση Εταιρικών Πόρων (Asset Management)

8.5.1. Καταγραφή Εξοπλισμού

Η VLP HELLAS SA να διατηρεί έναν ενημερωμένο κατάλογο με το πληροφοριακό και δικτυακό εξοπλισμό που στηρίζει την επιχειρηματική λειτουργία του Οργανισμού, το βαθμό κρισιμότητας του αλλά και τον αντίστοιχο Ιδιοκτήτη Πληροφοριών. Η διαδικασία της καταγραφής των πόρων του οργανισμού είναι σημαντικό τμήμα της διαδικασίας διαχείρισης κινδύνου. Ο κατάλογος πρέπει να είναι ανανεωμένος και να καταγράφονται σε αυτόν όλες οι αλλαγές που έχουν λάβει χώρα.

Οι πόροι που καταγράφονται κατά ελάχιστο είναι οι ακόλουθοι:

- **Πληροφοριακοί Πόροι (Software Assets)**: βάσεις δεδομένων, αρχεία δεδομένων, εφαρμογές, εργαλεία ανάπτυξης, servers κλπ.
- **Φυσικοί Πόροι**: υλικό υπολογιστών, εξοπλισμός τηλεπικοινωνιών, αποθηκευτικά μέσα κλπ.
- **Δικτυακός Εξοπλισμός**: μηχανισμοί προστασίας (firewalls, IDS), switches κλπ. (A_03-Αρχείο Καταγραφής Εταιρικών Πόρων-Asset Registry)

8.5.2. Αποδεκτή Χρήση των Πληροφοριακών Πόρων

Η VLP HELLAS SA πρέπει να ορίζει τους κανόνες για την αποδεκτή χρήση των πληροφοριών και των πληροφοριακών της συστημάτων, σύμφωνα με το βαθμό κρισιμότητάς τους. Σκοπός είναι η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και των συστημάτων και η αποτροπή επιβλαβών συμβάντων που μπορεί να προκύψουν από την κακή χρήση των παραπάνω. Όλοι οι χρήστες οφείλουν να είναι σε συμμόρφωση με τους κανόνες αυτούς και απαγορεύεται να προβαίνουν σε μη επιτρεπόμενες ενέργειες.

Πεδίο Εφαρμογής

Η παρούσα πολιτική αφορά όλες τις εταιρικές πληροφορίες είτε σε έντυπη είτε σε ηλεκτρονική μορφή και όλα τα πληροφοριακά συστήματα που στηρίζουν τις επιχειρηματικές λειτουργίες της VLP HELLAS SA.

Η πολιτική αυτή απευθύνεται σε όλα μέλη του προσωπικού και στους συνεργάτες της VLP HELLAS SA.

Γενικές Αρχές

Δικαιώματα και Υποχρεώσεις των Χρηστών

Όλοι οι χρήστες πρέπει να εφαρμόζουν και να τηρούν τη Πολιτική Ασφάλειας Πληροφοριών, τις υποστηρικτικές πολιτικές και διαδικασίες ασφάλειας και να εφαρμόζουν όλα τα ενδεικνυόμενα μέτρα, με σκοπό τη προστασία των πληροφοριών και πληροφοριακών συστημάτων (ΠΕΣ) της VLP HELLAS SA.

Όλο το προσωπικό (εξωτερικοί συνεργάτες και υπάλληλοι) πρέπει να αποκτά

πρόσβαση μόνο στους πληροφοριακούς πόρους που τους έχουν εκχωρηθεί για την διεξαγωγή των εργασιακών τους καθηκόντων. Οι χρήστες οφείλουν να χρησιμοποιούν τους πόρους που τους παρέχονται με ασφαλή και νόμιμο τρόπο.

Οι χρήστες δεν επιτρέπεται να αποκαλύπτουν διαβαθμισμένες πληροφορίες, τις οποίες χρησιμοποιούν ή/και επεξεργάζονται κατά τη διεξαγωγή των εργασιακών τους καθηκόντων. Επιπρόσθετα, οι χρήστες πρέπει να είναι ενήμεροι ότι τα δεδομένα και οι πληροφορίες οι οποίες δημιουργούνται κατά τη διάρκεια της εργασίας τους στον Οργανισμό, είναι ιδιοκτησία της VLP HELLAS SA.

Οι χρήστες δεν επιτρέπεται να υποκλέπτουν ή με οποιοδήποτε άλλο τρόπο να ανακαλύπτουν συνθηματικά, κρυπτογραφικά κλειδιά ή οποιοδήποτε άλλο μηχανισμό ελέγχου πρόσβασης ο οποίος θα μπορούσε να τους επιτρέψει μη εξουσιοδοτημένη πρόσβαση στα πληροφοριακά και δικτυακά συστήματα του Οργανισμού. Κάθε προσπάθεια μείωσης του επιπέδου ασφάλειας των πληροφοριακών συστημάτων απαγορεύεται αυστηρά.

Απαγορεύεται κάθε είδους χρήση, εγκατάσταση και αντιγραφή παράνομου λογισμικού στα πληροφοριακά συστήματα της VLP HELLAS SA.

Οι χρήστες δεν επιτρέπεται να εγκαθιστούν μη εξουσιοδοτημένο λογισμικό (οποιοδήποτε λογισμικό δεν έχει εγκατασταθεί από την ομάδα του IT Support), καθώς υπάρχει σοβαρός κίνδυνος το λογισμικό αυτό να είναι μολυσμένο με ιούς υπολογιστών, Trojan horses κλπ. το οποίο δύναται να βλάψει τις πληροφορίες και τα συστήματα του Οργανισμού.

Η χρήση των πληροφοριακών συστημάτων της VLP HELLAS SA παρέχεται στο προσωπικό της ως εργαλείο διεξαγωγής επιχειρηματικών δραστηριοτήτων. Η χρήση αυτών για προσωπικούς σκοπούς είναι επιτρεπτή μέσα σε ορισμένα πλαίσια, και επιτρέπεται όταν:

- Δε στοχεύει σε επίτευξη προσωπικού οφέλους του εργαζόμενου ή άλλης επιχειρηματικής οντότητας πλην της VLP HELLAS SA (εμπλοκή σε προσωπικές επιχειρηματικές δραστηριότητες του εργαζομένου, επιχειρήσεις με τις οποίες ο εργαζόμενος έχει οποιαδήποτε σχέση κερδοσκοπική ή μη κτλ)
- Δεν επηρεάζει την παραγωγικότητα των εργαζομένων
- Δεν αποσκοπεί σε εξυπηρέτηση πολιτικών-κομματικών συμφερόντων
- Δεν αντίκειται στην παρούσα και σε οποιαδήποτε άλλη πολιτική

Δικαιώματα και Υποχρεώσεις της VLP HELLAS SA

Η VLP HELLAS SA οφείλει να αναλύει κατά τη διάρκεια της πρόσληψης τις ευθύνες αναφορικά με την ασφάλεια των πληροφοριών. Οι ευθύνες αυτές πρέπει να αποτυπώνονται στο σχετικό συμβόλαιο εργασίας και να ελέγχονται κατά τη διάρκεια της συνεργασίας της VLP HELLAS SA και του χρήστη.

Η VLP HELLAS SA οφείλει να ενημερώνει όλους τους χρήστες του κατάλληλα για την Πολιτική Ασφάλειας Πληροφοριών και τις όποιες αλλαγές γίνονται σε αυτήν. Αναλυτικότερα, πρέπει να τους γνωστοποιεί τις διαδικασίες, τις νομικές ευθύνες, τους μηχανισμούς προστασίας και αποδεκτής χρήσης, βάσει του ρόλου τους, και να τους εκπαιδεύει για τη σωστή χρήση των πληροφοριακών συστημάτων του Οργανισμού, ώστε να ελαχιστοποιηθούν οι πιθανοί κίνδυνοι κατά της ασφάλειας τους.

Η VLP HELLAS SA διατηρεί το δικαίωμα να διενεργεί τακτικούς ή έκτακτους ελέγχους στα πληροφοριακά συστήματα για την τήρηση των πολιτικών, των διαδικασιών και

των μηχανισμών ασφάλειας. Τους ελέγχους τους πραγματοποιούν εξουσιοδοτημένα άτομα, και το προσωπικό οφείλει να συνεργαστεί για την ομαλή διεξαγωγή αυτών.

Προστασία Εταιρικών Πληροφοριών

Οι χρήστες κατά τη διαχείριση των συστημάτων και πληροφοριών του Οργανισμού πρέπει να συμμορφώνονται με το ισχύον νομοθετικό και κανονιστικό πλαίσιο και ειδικότερα με τις διατάξεις για την προστασία των προσωπικών δεδομένων.

Οι διαβαθμισμένες πληροφορίες είτε σε έντυπη είτε σε ηλεκτρονική μορφή πρέπει να αποθηκεύονται σε ασφαλείς τοποθεσίες όταν δεν χρησιμοποιούνται και ιδιαίτερα τις μη εργάσιμες ώρες.

Όλα τα έγγραφα τα οποία περιέχουν διαβαθμισμένες πληροφορίες και δεν είναι χρήσιμα, πρέπει να καταστρέφονται προσεκτικά, για παράδειγμα με τη χρήση ειδικών μηχανημάτων (shredder).

Όλοι οι υπάλληλοι της VLP HELLAS SA είναι υπεύθυνοι να «κλειδώνουν» τους σταθμούς εργασίας / φορητούς υπολογιστές όταν απομακρύνονται από αυτούς και να χρησιμοποιούν προστασία φύλαξης της οθόνης (screen saver).

Οι υπάλληλοι απαγορεύεται να αποκαλύπτουν σε τρίτους ή να δημοσιοποιούν πληροφορίες και δεδομένα του Οργανισμού τα οποία δεν προορίζονται για δημόσια χρήση. Ενδεικτικά:

- Πληροφορίες χρηματοοικονομικού περιεχομένου που δεν έχουν δημοσίως κοινοποιηθεί
- Επιχειρησιακά πλάνα και στρατηγικές
- Ερευνητικές εργασίες που διεξάγονται στο πλαίσιο των δραστηριοτήτων του Οργανισμού
- Πληροφορίες που σχετίζονται με συνδρομητές των υπηρεσιών που παρέχει ο Οργανισμός
- Πληροφορίες αναφορικά με τους εξωτερικούς συνεργάτες του Οργανισμού
- Κάθε πληροφορία, η οποία δεν έχει χαρακτηριστεί ότι προορίζεται για δημόσια χρήση

Αποδεκτή Χρήση Συνθηματικών

Όλοι οι χρήστες, ιδιαίτερα με προνομιούχα δικαιώματα (π.χ. administrator), πρέπει να χρησιμοποιούν καλές πρακτικές αναφορικά με την επιλογή και τη χρήση των συνθηματικών που χρησιμοποιούν για να αποκτήσουν πρόσβαση στα πληροφοριακά συστήματα του Οργανισμού. Κάθε χρήστης είναι υπεύθυνος για την ασφαλή χρήση του συνθηματικού του.

Τα συνθηματικά πρέπει να έχουν τουλάχιστον τα ακόλουθα χαρακτηριστικά:

- Να αποτελούνται τουλάχιστον από 8 χαρακτήρες
- Να περιέχουν αλφαριθμητικά
- Να περιέχουν σύμβολα

Τα συνθηματικά πρέπει να αλλάζουν ανά τακτά χρονικά διαστήματα, τουλάχιστον κάθε έξι μήνες. Όλοι οι χρήστες πρέπει να αλλάζουν το συνθηματικό τους μετά τη πρώτη φορά εισόδου (login) στα πληροφοριακά συστήματα (τερματικό, laptop κ.ά.).

Όλα τα συστημικά και προνομιούχα συνθηματικά (root, domain admin, application administration accounts) πρέπει να είναι διαφορετικά από το προεπιλεγμένο (default).

Σε περίπτωση αποχώρησης υπαλλήλου με προνομιακά δικαιώματα στα πληροφοριακά συστήματα του Οργανισμού, το συνθηματικό αλλάζει αμέσως.

Μη Αποδεκτή Χρήση Συνθηματικών

Οι χρήστες δεν πρέπει να καταγράφουν και να φυλάσσουν τα συνθηματικά τους σε εμφανή σημεία (post-it). Σε κάθε περίπτωση, το συνθηματικό πρέπει να θεωρείται εμπιστευτική πληροφορία. Οι χρήστες δεν πρέπει να αποστέλλουν τα συνθηματικά μέσω του ηλεκτρονικού ταχυδρομείου.
Οι χρήστες πρέπει να αποφεύγουν τη χρήση αυτόματης συμπλήρωσης (απομνημόνευσης) των συνθηματικών στους σταθμούς εργασίας ή/και στους φορητούς υπολογιστές.

Ασφαλής Καταστροφή Πληροφοριακών Πόρων

Όλες οι διαβαθμισμένες πληροφορίες είτε σε έντυπη είτε σε ηλεκτρονική μορφή, πρέπει να καταστρέφονται με ασφάλεια όταν πλέον δεν είναι χρήσιμες για τη λειτουργία του Οργανισμού, με σκοπό να αποφευχθεί η διαρροή τους.

8.5.3. Διαχείριση Αποθηκευτικών Μέσων και Εγγράφων

Η VLP HELLAS SA πρέπει να λάβει όλα τα απαραίτητα μέτρα για την προστασία των διαφόρων αποθηκευτικών μέσων (δίσκοι, ταινίες κ.ά.) και των εγγράφων που διατηρεί από πιθανές καταστροφές, κλοπή ή μη εξουσιοδοτημένη πρόσβαση.

Επίσης, ο Οργανισμός ακολουθεί επίσημες και καταγεγραμμένες διαδικασίες αναφορικά με την απόσυρση των αποθηκευτικών μέσων και των εγγράφων, ιδιαίτερα στην περίπτωση που περιέχουν ευαίσθητα δεδομένα, λαμβάνοντας υπόψη την υφιστάμενη νομοθεσία και το βαθμό κρισιμότητάς τους.

Τα θέματα που αφορούν την ασφάλεια των αποθηκευτικών μέσων και εγγράφων περιγράφονται παρακάτω.

Πεδίο Εφαρμογής

Η παρούσα πολιτική ισχύει για όλους τους χρήστες οι οποίοι στο πλαίσιο των εργασιακών τους καθηκόντων χειρίζονται έγγραφα ή/και αποθηκευτικά μέσα. Στην παρούσα πολιτική, αφαιρούμενα αποθηκευτικά μέσα θεωρούνται όλα όσα μπορούν να μετακινηθούν και να χρησιμοποιηθούν χωρίς να απαιτείται πρόσβαση στο εσωτερικό του συστήματος όπου είναι εγκατεστημένα

Γενικές Αρχές

Χρήση Αποθηκευτικών Μέσων και Εγγράφων

Σε όλα τα έγγραφα τα οποία περιέχουν εμπιστευτικές πληροφορίες, πρέπει να αναγράφεται κατάλληλα ο βαθμός κρισιμότητάς τους σε ευκρινές σημείο. Επιπρόσθετα, η VLP HELLAS SA πρέπει να τηρεί λίστα των εργαζομένων που έχουν πρόσβαση στα αρχεία υψηλά διαβαθμισμένων πληροφοριών.

Τα έγγραφα και τα αποθηκευτικά μέσα (π.χ. CDs, εξωτερικοί δίσκοι) που περιέχουν διαβαθμισμένες πληροφορίες πρέπει να αποθηκεύονται σε ασφαλείς χώρους όταν δεν είναι σε χρήση (π.χ. ντουλάπια με κλειδαριά, χρηματοκιβώτιο), ιδιαίτερα τις μη-

εργάσιμες ώρες, έτσι ώστε η πρόσβαση σε αυτά να είναι εφικτή μόνο από εξουσιοδοτημένους χρήστες.

Οι εμπιστευτικές πληροφορίες του Οργανισμού πρέπει να παράγονται σε έντυπη μορφή ή να αποθηκεύονται σε αποθηκευτικά μέσα, μόνο στο βαθμό που απαιτείται για την ικανοποίηση των επιχειρησιακών αναγκών του Οργανισμού.

Μεταφορά Αποθηκευτικών Μέσων και Εγγράφων

Η μεταφορά των αποθηκευτικών μέσων και εγγράφων, μεταξύ του Οργανισμού και εκτός του Οργανισμού χώρων, πρέπει να ακολουθεί επίσημες διαδικασίες ανάλογα με την κρισιμότητα των πληροφοριών που βρίσκονται αποθηκευμένες, και μόνο για την εξυπηρέτηση επιχειρησιακών αναγκών.

Για τις ανάγκες μεταφοράς αποθηκευτικών μέσων και εγγράφων, πρέπει να υπάρχει λίστα αποδεκτών εταιρειών ταχυδρομείου (π.χ. courier). Οι εταιρείες αυτές πρέπει να έχουν συμβατικά δεσμευτεί ότι θα διασφαλίζουν την αξιοπιστία και την εμπιστευτικότητα των παρεχόμενων υπηρεσιών. Αυτή η λίστα πρέπει να διατηρείται από την αρμόδια οργανωτική μονάδα του Οργανισμού.

Ασφαλής Χρήση Φορητών Υπολογιστών και Φορητών Αποθηκευτικών Μέσων

Η χρήση προσωπικών φορητών υπολογιστών και φορητών αποθηκευτικών μέσων δεν είναι επιτρεπτή. Οι χρήστες μπορούν να χρησιμοποιούν φορητούς υπολογιστές και μέσα που τους παρέχει ο Οργανισμός στο πλαίσιο της διεξαγωγής των εργασιακών τους καθηκόντων.

Η παροχή φορητών υπολογιστών και μέσων αποσκοπεί στην εκπλήρωση των εργασιακών καθηκόντων των χρηστών. Οι υπάλληλοι της VLP HELLAS SA δεν επιτρέπεται να δανείζουν τον εξοπλισμό που τους παρέχεται ή να επιτρέπουν τη χρήση αυτών από μη εξουσιοδοτημένα άτομα. Ο εκάστοτε ιδιοκτήτης του φορητού υπολογιστή ή/και του φορητού αποθηκευτικού μέσου είναι υπεύθυνος για κάθε πιθανή ζημιά που θα προκληθεί από μη εξουσιοδοτημένους χρήστες.

Η VLP HELLAS SA πρέπει να διατηρεί μια ενημερωμένη λίστα με τους υπολογιστές, τα φορητά αποθηκευτικά μέσα και με τα στοιχεία των υπαλλήλων στους οποίους έχουν παραχωρηθεί. Η VLP HELLAS SA διατηρεί το δικαίωμα να προβεί σε ελέγχους, έτσι ώστε να εξασφαλιστεί η αποδεκτή και σύμφωνη χρήση με τα εργασιακά καθήκοντα του υπαλλήλου.

Η αποθήκευση εμπιστευτικών πληροφοριών στους φορητούς υπολογιστές και στα φορητά μέσα αποθήκευσης θα πρέπει να αποφεύγεται. Οι πληροφορίες αυτές πρέπει να αποθηκεύονται σε εξυπηρετητές αρχείων (server) του Οργανισμού ή σε τοπικούς σκληρούς δίσκους. Ωστόσο, εφόσον υπάρχει συγκεκριμένη ανάγκη, οι πληροφορίες θα πρέπει να κρυπτογραφούνται.

Οι χρήστες πρέπει να αποφεύγουν να συνδέουν τα φορητά αποθηκευτικά μέσα σε μη-εταιρικό εξοπλισμό, καθώς υπάρχει περίπτωση να μεταφέρουν ιούς στο δίκτυο του Οργανισμού. Σε μια τέτοια περίπτωση, θα πρέπει να ελέγχουν τα μέσα πριν τα συνδέσουν στο δίκτυο του Οργανισμού.

Οι χρήστες είναι υπεύθυνοι για τη φυσική προστασία των φορητών υπολογιστών και μέσων που τους έχουν παραχωρηθεί. Οφείλουν να επιβεβαιώνουν πως τα μέσα δεν μένουν αφύλακτα χωρίς την επιτήρηση τους. Σε τέτοιες περιπτώσεις λαμβάνουν τα κατάλληλα μέτρα (π.χ. φύλαξη οθόνης με συνθηματικό, φύλαξη σε κλειδωμένους χώρους κ.ά.).

Οι υπολογιστές δεν πρέπει να παραμένουν αφύλακτοι και με το χρήστη να είναι συνδεδεμένος. Οι χρήστες πάντα «κλειδώνουν» το φορητό υπολογιστή και να τερματίζουν τις συνδέσεις (log-off) όταν υπάρχει ανάγκη απομάκρυνσης από αυτό.

Οι χρήστες πρέπει να αποφεύγουν να αποθηκεύουν τα συνθηματικά τους μέσα στους φορητούς υπολογιστές. Ως αποτέλεσμα, σε περίπτωση μη εξουσιοδοτημένης πρόσβασης, δε θα είναι εφικτή η πρόσβαση σε άλλους πόρους του χρήστη (για παράδειγμα, στο δίκτυο του οργανισμού ή στο προσωπικό ηλεκτρονικό ταχυδρομείο του χρήστη).

Οι χρήστες είναι υπεύθυνοι να ενημερώνουν το αντιβιοτικό λογισμικό (antivirus) που είναι εγκατεστημένο στο φορητό υπολογιστή. Σε περίπτωση αντιμετώπισης προβλήματος, πρέπει να ενημερώσουν άμεσα την ομάδα του IT Support.

Σε περίπτωση απώλειας/ κλοπής του φορητού υπολογιστή ή των φορητών μέσων, ο χρήστης πρέπει να ενημερώσει άμεσα τον Προϊστάμενό του και την αστυνομία.

Κατά την αποχώρηση του χρήστη από τον Οργανισμό, βεβαιώνεται η παράδοση των φορητών υπολογιστών και αποθηκευτικών μέσων που είχε στη κατοχή του.

Όλοι οι φορητοί υπολογιστές που έχουν επιστραφεί, πρέπει να υποβάλλονται τουλάχιστον σε μια διαδικασία format, πριν να δοθούν σε νέο χρήστη.

Καταστροφή Αποθηκευτικών Μέσων και Εγγράφων

Σε περίπτωση που κάποιο επαναχρησιμοποιούμενο αποθηκευτικό μέσο πρόκειται να αλλάξει χρήση ή δεν απαιτείται πλέον η διατήρηση των αποθηκευμένων πληροφοριών του, τότε πρέπει να διαγράφονται με ασφαλή τρόπο όλα τα περιεχόμενά του.

Όλα τα διαβαθμισμένα έγγραφα τα οποία βρίσκονται σε έντυπη μορφή, πρέπει να καταστρέφονται ασφαλώς με τη χρήση κατάλληλων μηχανημάτων (π.χ. shredder).

Οι Ιδιοκτήτες Συστημάτων πρέπει να εξασφαλίζουν ότι πριν τη καταστροφή των αποθηκευτικών μέσων, τα δεδομένα και το λογισμικό που βρίσκονται αποθηκευμένα σε αυτά έχουν αφαιρεθεί. (A_05 - Αρχείο Καταστροφής Διαβαθμισμένων Εγγράφων & Αποθηκευτικών Μέσων)

8.6 .Πολιτική Προσωπικού

Το προσωπικό και οι συνεργάτες της VLP HELLAS SA είναι υπεύθυνοι για την προστασία και την αποδεκτή χρήση των πληροφοριών και των πληροφοριακών συστημάτων που ανήκουν στην VLP HELLAS SA και πρέπει να απέχει από κάθε ενέργεια που μπορεί να θέσει σε κίνδυνο την ασφάλεια των πόρων. Το προσωπικό και οι συνεργάτες της VLP HELLAS SA πρέπει να υπογράφουν δηλώσεις για την τήρηση εχεμύθειας (non-disclosure agreements) κατά την έναρξη της συνεργασίας τους με τον Οργανισμό.

Η ευθύνη και ο έλεγχος τήρησης της ασφάλειας καθώς και ο συντονισμός των ενεργειών που σχετίζονται με την ασφάλεια σε όλο το εύρος του Οργανισμού, ξεκινά από τη Διοίκηση και εξαπλώνεται σε όλες τις βαθμίδες της ιεραρχίας του προσωπικού (top-down).

Τα θέματα ασφάλειας αναφορικά με το προσωπικό περιγράφονται παρακάτω.

Πεδίο Εφαρμογής

Η παρούσα πολιτική αφορά όλο το ανθρώπινο δυναμικό της VLP HELLAS SA

Γενικές Αρχές

Γενικές Αρχές Πριν τη Πρόσληψη Νέου Προσωπικού

Η VLP HELLAS SA πρέπει να επιλέγει κατάλληλα καταρτισμένο και εκπαιδευμένο προσωπικό για την υποστήριξη της ομαλής λειτουργίας και της ικανοποίησης των απαιτήσεων ασφαλείας του Οργανισμού (σε ότι αφορά νευραλγικές θέσεις).

Κατά την υποβολή αιτήσεων από τους υποψήφιους για μία θέση / υλοποίηση έργου, η Διεύθυνση Ανθρώπινου Δυναμικού θα πρέπει να ελέγχει τα όσα αναφέρονται σε αυτές. Θα πρέπει να ελέγχονται, όπου είναι δυνατόν, τουλάχιστον τα παρακάτω:

Τα στοιχεία που αναφέρονται στο βιογραφικό σημείωμα του υποψηφίου είναι ακριβή

Ο υποψήφιος κατέχει τους τίτλους που αναφέρει

Περιλαμβάνεται αποδεικτικό της ταυτότητας του υποψηφίου

Η Διεύθυνση Ανθρώπινου Δυναμικού είναι υπεύθυνη να εξασφαλίσει πως ο Υποψήφιος εργαζόμενος ή εξωτερικός συνεργάτης έχει λάβει γνώση της υπάρχουσας Πολιτικής Ασφαλείας του Οργανισμού.

Η Διεύθυνση Ανθρώπινου Δυναμικού είναι υπεύθυνη να εξασφαλίσει πως μεταξύ του Οργανισμού και του υποψήφιου εργαζόμενου υπογράφεται μια δήλωση εμπιστευτικότητας, πριν δοθεί πρόσβαση στα πληροφοριακά συστήματα του Οργανισμού. Οι νομικές ευθύνες του υπαλλήλου όπως και τα δικαιώματά του πρέπει να αναφέρονται με σαφήνεια στο συμβόλαιό του (E_04- Βεβαίωση Εμπιστευτικότητας).

Γενικές Αρχές κατά τη Διάρκεια της Πρόσληψης

Ο εκάστοτε προϊστάμενος του χρήστη είναι υπεύθυνος να ενημερώσει κατάλληλα τους νεοεισερχόμενους υπαλλήλους αναφορικά με την Πολιτική Ασφάλειας Πληροφοριών, τις επιμέρους πολιτικές και διαδικασίες ασφάλειας. Είναι σημαντικό να επισημανθεί, πως η συμμόρφωση με τις πολιτικές, τις διαδικασίες και τους μηχανισμούς ασφαλείας είναι υποχρεωτική για όλους τους υπαλλήλους της VLP HELLAS SA.

Η Διεύθυνση Ανθρώπινου Δυναμικού είναι υπεύθυνη να τηρεί ενημερωμένο αρχείο για όλο το δυναμικό της VLP HELLAS SA. Το αρχείο πρέπει να περιλαμβάνει ακριβείς και ενημερωμένες πληροφορίες αναφορικά με το ρόλο και τις αρμοδιότητες του εργαζόμενου μέσα στον Οργανισμό.

Η VLP HELLAS SA οφείλει να ακολουθεί επίσημες διαδικασίες για τον ασφαλή χειρισμό των προσωπικών δεδομένων των υπαλλήλων (π.χ. οικονομικά στοιχεία, ιατρικά στοιχεία).

Όλοι οι πόροι που παρέχονται στους υπαλλήλους / συνεργάτες για τη διεξαγωγή των εργασιακών τους καθηκόντων (π.χ. φορητοί υπολογιστές, κάρτες εισόδου κ.ά.) πρέπει να καταγράφονται. Οι χρήστες οφείλουν να υπογράφουν μια βεβαίωση παραλαβής των πόρων.

Γενικές Αρχές κατά τη Λήξη της Εργασίας / Συνεργασίας

Σε κάθε περίπτωση όπου τερματίζεται η συνεργασία του χρήστη με τον Οργανισμό, η Διεύθυνση Ανθρωπίνου Δυναμικού σε συνεργασία με τους προϊσταμένους των χρηστών θα πρέπει να φροντίσουν άμεσα για τις παρακάτω ενέργειες:

- Την άμεση ανάκληση όλων των δικαιωμάτων φυσικής και λογικής πρόσβασης που τους είχαν παραχωρηθεί.
- Την επιστροφή κάθε πληροφορίας ή εξοπλισμού που ανήκει στην VLP HELLAS SA

Δεν επιτρέπεται στους υπαλλήλους / συνεργάτες να απομακρύνουν ή να διατηρούν πληροφορίες της VLP HELLAS SA μετά την λήξη της συνεργασίας με τον Οργανισμό. Όλες οι πληροφορίες που τηρούνται από τον εργαζόμενο / συνεργάτη ή είναι στην κατοχή του κατά τη διάρκεια της απασχόλησής του, θα πρέπει να παραδίδονται στο προϊστάμενό του πριν την αποχώρησή του. Εξαίρεση για τη μη εφαρμογή της παραπάνω πολιτικής αποτελούν προσωπικά αντίγραφα δημόσιων πληροφοριών, και προσωπικά αντίγραφα ηλεκτρονικής αλληλογραφίας.

Όλοι οι χρήστες κατά τη λήξη της εργασιακής τους σχέσης με τον Οργανισμό οφείλουν να επιστρέψουν όλα τα περιουσιακά στοιχεία της VLP HELLAS SA που τους παραχωρήθηκαν για την εκτέλεση της εργασίας τους, όπως φορητούς υπολογιστές, λογισμικό, κλειδιά, εγχειρίδια, κλπ.

8.7 .Ενημέρωση και Εκπαίδευση Ασφάλειας

Η VLP HELLAS SA οφείλει να ενημερώνει και να εκπαιδεύει κατάλληλα όλο το προσωπικό και τους συνεργάτες της σε θέματα ασφάλειας πληροφοριών. Η εκπαίδευση έχει ως στόχο να ενημερώσει τους χρήστες όσον αφορά στην Πολιτική Ασφάλειας, τις διαδικασίες ασφάλειας αλλά και στις πρακτικές ασφάλειας που εφαρμόζονται στον Οργανισμό με σκοπό να τα εφαρμόζουν κατάλληλα στη καθημερινή τους εργασία εντός και εκτός των γραφείων της VLP HELLAS SA.

Με τον τρόπο αυτό μπορούν να ελαχιστοποιηθούν οι πιθανοί κίνδυνοι κατά της ασφάλειας των πληροφοριών. Οι εργαζόμενοι που είναι ευαισθητοποιημένοι και ενήμεροι σε θέματα ασφάλειας πληροφοριών αποτελούν ένα από τα καλύτερα μέτρα προστασίας για την ασφάλεια των πληροφοριών και των υποδομών της VLP HELLAS SA.

Ο στόχος της ενημέρωσης είναι να εξασφαλιστεί ότι όλοι οι χρήστες που έχουν πρόσβαση στα πληροφοριακά συστήματα και στις πληροφορίες της VLP HELLAS SA αντιλαμβάνονται την ανάγκη για ασφάλεια και κατανοούν την προσωπική ευθύνη που οι ίδιοι φέρουν και επίσης έχουν γνώση των βασικών αρχών που πρέπει να ακολουθούνται.

Τα θέματα αναφορικά με την εκπαίδευση του προσωπικού περιγράφονται παρακάτω.

Εκπαίδευση / Ενημέρωση του Προσωπικού

Η Διεύθυνση Ανθρώπινου Δυναμικού σε συνεργασία με τον Υπεύθυνο Ασφάλειας, θα πρέπει να φροντίζει έτσι ώστε η εκπαίδευση σε θέματα ασφάλειας πληροφοριών:

- Να είναι συνεχής
- Να παρέχεται σε όλους τους εργαζόμενους
- Να είναι έτσι σχεδιασμένη ώστε να προωθεί το αίσθημα προσωπικής ευθύνης για να αυξηθεί η αποτελεσματικότητα
- Να προσφέρει στο ανθρώπινο δυναμικό τη γνώση, έτσι ώστε να μπορούν να διεκπεραιώνουν αποτελεσματικά τα καθήκοντα τους ως προς την ασφάλεια

Η Διεύθυνση Ανθρωπίνου Δυναμικού σε συνεργασία με τον Υπεύθυνο Ασφάλειας θα πρέπει να ενημερώνουν και να εξασφαλίζουν την αποδοχή των νέων-προσληφθέντων εργαζομένων / συνεργατών ως προς την τήρηση της Πολιτικής Ασφάλειας Πληροφοριών, των μηχανισμών ασφάλειας και των σχετικών διαδικασιών. Η ενημέρωση αυτή θα πρέπει να υλοποιείται μόλις προσλαμβάνεται ο εργαζόμενος / ξεκινά η συνεργασία με τον εξωτερικό συνεργάτη, με τους παρακάτω τρόπους:

- Ενημέρωση σε θέματα ασφάλειας πληροφοριών
- Προστασία των πληροφοριών του Οργανισμού
- Συμμόρφωση με το νομικό πλαίσιο
- Πολιτικές και διαδικασίες ασφάλειας

Η παροχή εκπαίδευσης και ενημέρωσης αναφορικά με θέματα ασφάλειας πρέπει να είναι προσαρμοσμένη στις ανάγκες του ρόλου και των αρμοδιοτήτων των χρηστών (π.χ. διαχειριστές συστημάτων).

8.8 .Τρίτες Οντότητες

Η VLP HELLAS SA πρέπει να διασφαλίσει πως οι εξωτερικοί της συνεργάτες (προμηθευτές, συνεργάτες, σύμβουλοι κ.ά.) συμμορφώνονται και εφαρμόζουν τα όσα ορίζει η Πολιτική Ασφάλειας Πληροφοριών και έχουν πρόσβαση στους πόρους της VLP HELLAS SA μόνο στα πλαίσια των εργασιακών τους καθηκόντων και για κανένα άλλο λόγο.

Σε κάθε περίπτωση συμφωνίας μεταξύ της VLP HELLAS SA και της Τρίτης Οντότητας όπου προβλέπεται η παροχή πρόσβασης σε διαβαθμισμένα, ευαίσθητα ή απόρρητα δεδομένα, της VLP HELLAS SA πρέπει να λάβει τα απαραίτητα μέτρα για τη διασφάλιση της εμπιστευτικότητας των πληροφοριών και να υπογράφονται ειδικές συμβάσεις και συμφωνίες για την τήρηση της εχεμύθειας των πληροφοριών.

Οι βασικές αρχές ασφάλειας αναφορικά με τις Τρίτες Οντότητες περιγράφονται παρακάτω.

Πεδίο Εφαρμογής

Η παρούσα πολιτική ασφάλειας αφορά σε όλα τα τρίτα μέρη (π.χ. προμηθευτές, εξωτερικοί συνεργάτες, υπεργολάβοι) με τα οποία συνεργάζεται η VLP HELLAS SA, και στο πλαίσιο των εργασιακών τους καθηκόντων αποκτούν πρόσβαση στις πληροφορίες και στα πληροφοριακά συστήματα του Οργανισμού.

Γενικές Αρχές

Διαχείριση Τρίτων Μερών

Κάθε συνεργασία της VLP HELLAS SA με εξωτερικούς συνεργάτες πρέπει να υποστηρίζεται από τις κατάλληλες συμβάσεις. Οι απαιτήσεις ασφάλειας, οι υποχρεώσεις των εμπλεκομένων μερών και οι πειθαρχικές κυρώσεις που θα εφαρμοστούν σε περίπτωση μη συμμόρφωσης πρέπει να καταγράφονται, μεταξύ άλλων, με σαφήνεια στις συμβάσεις αυτές.

Βασικοί όροι των συμβάσεων είναι:

- Διασφάλιση του απορρήτου των επικοινωνιών με στόχο τη διατήρηση της εμπιστευτικότητας και ακεραιότητας των δεδομένων επικοινωνίας κατά την επεξεργασία αυτών και οριστική διαγραφή και καταστροφή αυτών μετά τη λήξη της συνεργασίας.
- Αποδοχή της υποχρέωσης για τήρηση των μέτρων ασφάλειας για τη διασφάλιση του απορρήτου των επικοινωνιών.

Σε περίπτωση όπου απαιτείται πρόσβαση σε εξοπλισμό ή λογισμικό το οποίο παρέχει πρόσβαση σε εμπιστευτικά δεδομένα, πρέπει να υπογράφεται σχετική δήλωση εμπιστευτικότητας, η οποία αποτελεί αναπόσπαστο τμήμα της σύμβασης.

Όλες οι συμβάσεις εργασίας, έργου και οι συμβάσεις εμπιστευτικότητας πρέπει να αναθεωρούνται από το νομικό σύμβουλο της VLP HELLAS SA πριν υπογραφούν.

Η VLP HELLAS SA οφείλει να εφαρμόζει όλα τα απαραίτητα μέτρα για την προστασία της εμπιστευτικότητας και της ακεραιότητας των πληροφοριών κατά τη συνεργασία με τους εξωτερικούς συνεργάτες.

Η VLP HELLAS SA οφείλει να επανεξετάζει τις συμφωνίες εμπιστευτικότητας ανά τακτά χρονικά διαστήματα και να γνωμοδοτεί για την επάρκεια των όρων της

σύμβασης σε σχέση με την ασφάλεια των πληροφοριών.

Πρόσβαση Τρίτων Μερών

Κατά την παροχή πρόσβασης των εξωτερικών συνεργατών στους πληροφοριακούς πόρους της VLP HELLAS SA, πρέπει να εξετάζονται όλοι οι ενδεχόμενοι κίνδυνοι και να λαμβάνονται όλα τα απαραίτητα μέτρα ασφάλειας. Σκοπός είναι η προστασία των πληροφοριών και η αδιάλειπτη λειτουργία των συστημάτων της VLP HELLAS SA.

Ο βαθμός πρόσβασης και οι υπηρεσίες που παρέχονται σε εξωτερικούς συνεργάτες θα πρέπει να περιορίζονται στις απολύτως απαραίτητες, προκειμένου να επιτελούνται οι επιχειρηματικές διεργασίες. Τα δικαιώματα πρόσβασης των χρηστών στα πληροφοριακά συστήματα θα πρέπει να καθορίζονται βάσει της ανάγκης γνώσης (need-to-know).

Τα δικαιώματα πρόσβασης πρέπει να αναθεωρούνται όταν οι ρόλοι, οι ανάγκες ή το αντικείμενο εργασίας μεταβάλλονται. Η παραπάνω διαδικασία ακολουθείται και στην περίπτωση ανάκλησης των δικαιωμάτων πρόσβασης.

Η VLP HELLAS SA οφείλει να επανεξετάζει περιοδικά τις διασυνδέσεις και τα δικαιώματα πρόσβασης που έχουν χορηγηθεί στους εξωτερικούς συνεργάτες και να ανακαλεί όσα κρίνεται ότι δεν εξυπηρετούν πλέον τις επιχειρησιακές της ανάγκες.

Υποχρεώσεις Τρίτων Μερών

Τα τρίτα μέρη οφείλουν να γνωρίζουν και να εφαρμόζουν την Πολιτική Ασφάλειας Πληροφοριών της VLP HELLAS SA καθώς και τις σχετικές πολιτικές, διαδικασίες και πρότυπα που πρόκειται να ακολουθήσουν στα πλαίσια της συνεργασίας τους.

Τα τρίτα μέρη σε καμία περίπτωση δεν έχουν το δικαίωμα να αποκαλύψουν εσωτερικά ή εμπιστευτικά δεδομένα της VLP HELLAS SA.

Τα τρίτα μέρη είναι υποχρεωμένα να διατηρούν την εμπιστευτικότητα και την ακεραιότητα των δεδομένων στα οποία αποκτούν πρόσβαση στα πλαίσια της συνεργασίας τους με την VLP HELLAS SA.

Τα τρίτα μέρη δεν έχουν την άδεια να παραχωρούν τα δικαιώματα πρόσβασης και τα προνόμια που τους έχουν χορηγηθεί για τη χρήση των πληροφοριών και πληροφοριακών συστημάτων σε άλλα τρίτα μέρη. Σε περίπτωση που απαιτείται κάτι τέτοιο, θα πρέπει να υπογράφεται αντίστοιχη σύμβαση μεταξύ της VLP HELLAS SA και του συγκεκριμένου εξωτερικού συνεργάτη.

8.9 .Φυσική Ασφάλεια

Η VLP HELLAS SA εφαρμόζει όλα τα απαραίτητα μέτρα για την προστασία των εγκαταστάσεων του Οργανισμού, ιδιαίτερα στις περιπτώσεις όπου στεγάζεται κρίσιμος εξοπλισμός ο οποίος υποστηρίζει τις λειτουργίες του.

Οι πληροφοριακοί πόροι της VLP HELLAS SA πρέπει να προστατεύονται κατάλληλα έτσι ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση σε αυτούς και η αδιάλειπτη λειτουργία τους. Σκοπός είναι η πρόληψη της απώλειας και των ζημιών των πόρων και της διακοπής των επιχειρησιακών δραστηριοτήτων.

Τα θέματα της φυσικής ασφάλειας περιγράφονται παρακάτω:

Πεδίο Εφαρμογής

Το εύρος της συγκεκριμένης πολιτικής καλύπτει τις κεντρικές εγκαταστάσεις της VLP HELLAS SA. Η πολιτική απευθύνεται σε όλο το προσωπικό και τους εξωτερικούς συνεργάτες που αποκτούν πρόσβαση στις κεντρικές εγκαταστάσεις της VLP HELLAS SA στο πλαίσιο διεξαγωγής των εργασιακών τους καθηκόντων.

Γενικές Αρχές

Ασφάλεια Εγκαταστάσεων

Η VLP HELLAS SA οφείλει να ορίσει ασφαλείς χώρους εντός των εγκαταστάσεών της, στους οποίους εγκαθίστανται τα ΠΕΣ. Οι χώροι αυτοί, πρέπει να προστατεύονται με μηχανισμούς ασφάλειας όπως συστήματα ελεγχόμενης πρόσβασης (π.χ κάρτες ελεγχόμενης εισόδου). Στην περίπτωση πρόσβασης συνεργατών ή άλλων επισκεπτών στους χώρους, αυτοί θα πρέπει να συνοδεύονται από εξουσιοδοτημένο εργαζόμενο σε όλο το διάστημα παραμονής τους. Όλα τα μέτρα (π.χ. χρήση κάμερας, συναγερμού) που εφαρμόζει ο Οργανισμός για τη προστασία των εγκαταστάσεών του, όπου στεγάζει τα πληροφοριακά του συστήματα, πρέπει να είναι σύμφωνα με το ισχύον νομικό και κανονιστικό πλαίσιο.

Το προσωπικό της VLP HELLAS SA δεν πρέπει να παραβιάζει τους μηχανισμούς φυσικής ασφάλειας που υλοποιεί η VLP HELLAS SA για τη προστασία των χώρων όπου βρίσκονται τα πληροφοριακά συστήματα.

Ασφάλεια Εξοπλισμού

Τα πληροφοριακά συστήματα πρέπει να προστατεύονται φυσικά από κινδύνους ασφάλειας και περιβαλλοντικές απειλές. Η προστασία τους είναι απαραίτητη, προκειμένου να ελαχιστοποιηθεί ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης, απώλειας ή καταστροφής των πληροφοριών.

Η Διεύθυνση Ανθρώπινου Δυναμικού είναι υπεύθυνη να ελέγχει πως τα συστήματα πυρασφάλειας φυλάσσονται σε κανονικές συνθήκες, έτσι ώστε σε περίπτωση που υπάρξει εκδήλωση πυρκαγιάς να είναι αποτελεσματικά.

Τα καλώδια παροχής ρεύματος, τηλεπικοινωνιών και μεταφοράς δεδομένων θα πρέπει να προστατεύονται από φυσική φθορά και καταστροφή.

Δεν επιτρέπεται η κατανάλωση φαγητού και ποτού κοντά σε κρίσιμο εξοπλισμό της VLP HELLAS SA (π.χ. Computer Room).

Έλεγχος Φυσική Πρόσβασης

Η VLP HELLAS SA πρέπει να καθορίσει τους κανόνες και τη διαδικασία φυσικής εισόδου στα κτίρια και στους επιμέρους χώρους της, όπου βρίσκονται τα πληροφοριακά συστήματα.

Η Διεύθυνση Ανθρώπινου Δυναμικού είναι υπεύθυνη για την ενημέρωση του προσωπικού αναφορικά με τους κανόνες και τις διαδικασίες φυσικής εισόδου που πρέπει να τηρούνται.

Η πρόσβαση των εξωτερικών συνεργατών και των επισκεπτών στους χώρους του

Οργανισμού είναι επιτρεπτή για επιχειρησιακούς λόγους και μόνο. Οι εξωτερικοί συνεργάτες και οι επισκέπτες πρέπει να συνοδεύονται από το εξουσιοδοτημένο προσωπικό της VLP HELLAS SA κατά τη διάρκεια της παρουσίας τους στους χώρους του Οργανισμού, ιδιαίτερα στην περίπτωση των διαβαθμισμένων περιοχών. Ενδεικτικά, και όχι περιοριστικά, ο όρος επισκέπτη περιλαμβάνει πρώην υπαλλήλους, διανομείς, κατασκευαστές κ.ά.

8.10 .Προστασία του Δικτύου

Η VLP HELLAS SA πρέπει να αναπτύσσει και να υλοποιεί όλους τους απαραίτητους μηχανισμούς για την ασφάλεια της δικτυακής της υποδομής. Σκοπός είναι να προστατευθούν τόσο τα δεδομένα που μεταδίδονται μέσω του δικτύου όσο και ο δικτυακός εξοπλισμός από μη εξουσιοδοτημένη πρόσβαση και φυσικές καταστροφές.

Τα θέματα της ασφάλειας του δικτύου περιγράφονται παρακάτω

Πεδίο Εφαρμογής

Η παρούσα πολιτική πρέπει να λαμβάνεται υπόψη κατά το σχεδιασμό, αλλά και την υλοποίηση και λειτουργία του δικτύου του Οργανισμού. Η παρούσα πολιτική απευθύνεται σε όλο το προσωπικό της VLP HELLAS SA, και ιδιαίτερα στους διαχειριστές του δικτύου του Οργανισμού.

Γενικές Αρχές

Σχεδιασμός Δικτύου & Διαχείριση και Λειτουργία Δικτύου

Ο σχεδιασμός του δικτύου της VLP HELLAS SA πρέπει να λαμβάνει υπόψη και να ικανοποιεί τις επιχειρησιακές απαιτήσεις δικτύωσης (π.χ. ταχύτητα, εύρος ζώνης) του Οργανισμού.

Ο σχεδιασμός και γενικά όλες οι πληροφορίες αναφορικά με τη διαμόρφωση του δικτύου του Οργανισμού (π.χ. σχεδιάγραμμα δικτύου) πρέπει να είναι κατάλληλα διαβαθμισμένες σύμφωνα με το «Ε_07-Σχήμα Διαβάθμισης Πληροφοριών». Οι πληροφορίες πρέπει να τηρούνται καταγεγραμμένες από τον Υπεύθυνο Ασφαλείας.

Οι αρμοδιότητες του προσωπικού που ασχολείται με τη λειτουργία και τη συντήρηση του δικτύου πρέπει να είναι σαφώς ορισμένες.

Αρχές Λειτουργίας Συστημάτων Προστασίας του Δικτύου

Κατά την διαμόρφωση των συστημάτων προστασίας δικτύου πρέπει να λαμβάνονται υπόψη όλοι οι κίνδυνοι όπως προκύπτουν κατά τη διεξαγωγή αποτίμησης κινδύνων. Η διαμόρφωση των συστημάτων προστασίας πρέπει να επανεξετάζεται και να τροποποιείται, εάν αυτό κρίνεται απαραίτητο, κάθε φορά που προκύπτουν νέες απειλές και αδυναμίες.

Τα συστήματα προστασίας του δικτύου πρέπει να είναι ενεργοποιημένα κάθε μέρα, 24 ώρες. Σε περίπτωση που χρειάζεται να διακοπεί η λειτουργία τους, πρέπει πρώτα να ενημερώνονται όλα τα μέρη του προσωπικού που θα επηρεαστούν άμεσα.

Η βασική πολιτική των συστημάτων firewall, είναι να μην επιτρέπουν τη ροή κανενός είδους δεδομένων για τα οποία δεν έχει δοθεί προηγουμένως η απαραίτητη έγκριση από τη VLP

HELLAS SA (default deny stance).

Έλεγχος Λειτουργίας του Δικτύου

Ο Οργανισμός πρέπει να διενεργεί περιοδικούς ελέγχους ασφάλειας του δικτύου, έτσι ώστε να εξασφαλίζεται η αποδεκτή χρήση του και η προστασία των πληροφοριών και των πληροφοριακών συστημάτων. Οι έλεγχοι διεξάγονται από εξουσιοδοτημένο προσωπικό του Οργανισμού ή/και από κατάλληλα επιλεγμένους εξωτερικούς συνεργάτες.

Στο πλαίσιο διεξαγωγής των ελέγχων, το εμπλεκόμενο προσωπικό μπορεί να έχει πρόσβαση σε όσες πληροφορίες κρίνονται απαραίτητες για τη διεξαγωγή του ελέγχου (διαγράμματα δικτύων, διαμόρφωση εξοπλισμού κλπ).

Ο έλεγχος του δικτύου πρέπει να περιλαμβάνει διεθνώς αποδεκτές πρακτικές ελέγχου δικτύων δεδομένων, όπως penetration testing, vulnerability assessment.

Ο έλεγχος του δικτύου μπορεί να κινηθεί ύστερα από συμπλήρωση της «Φ_03-Φόρμας Αίτησης Ψηφιακού Ελέγχου» και αποστολής της στον Υπεύθυνο Ασφάλειας.

8.11 .Ασφάλεια κατά την Ανάπτυξη/ Απόκτηση Συστημάτων

Η ασφάλεια αποτελεί μία σημαντική παράμετρο αξιολόγησης, η οποία εξετάζεται και λαμβάνεται σοβαρά υπόψη κατά την προμήθεια ή την ανάπτυξη των πληροφοριακών συστημάτων.
Το πλαίσιο και οι κανόνες διαχείρισης και εφαρμογής της ασφάλειας πληροφοριών υιοθετείται τόσο κατά την προμήθεια των πληροφοριακών συστημάτων της VLP HELLAS SA, όσο και κατά τον σχεδιασμό, την ανάπτυξή και τη λειτουργία τους, σύμφωνα με τις καταγεγραμμένες πολιτικές, διαδικασίες, πρότυπα και οδηγίες.

Τα θέματα ασφάλειας που προκύπτουν κατά την ανάπτυξη, την απόκτηση και τη λειτουργία των πληροφοριακών συστημάτων περιγράφονται παρακάτω.

Πεδίο Εφαρμογής

Η παρούσα πολιτική απευθύνεται σε όλα τα πληροφοριακά συστήματα της VLP HELLAS SA. Ως πληροφοριακά συστήματα θεωρούνται όλες οι υποδομές του Οργανισμού, όπως εφαρμογές, λειτουργικά συστήματα, στοιχεία δικτύου (network elements) και πλατφόρμες.

Γενικές Αρχές

Για κάθε πληροφοριακό σύστημα (εφαρμογή, βάση δεδομένων, λειτουργικό σύστημα,δίκτυο κ.ά.) της VLP HELLAS SA, θα πρέπει να ορίζονται τουλάχιστον οι:

- Ιδιοκτήτης Συστήματος, ο οποίος θα έχει την συνολική ευθύνη σωστής λειτουργίας του πληροφοριακού συστήματος.
- Διαχειριστής Συστήματος, ο οποίος θα έχει την ευθύνη της καθημερινής

διαχείρισης και συντήρησης του συστήματος καθώς και της καθημερινής παρακολούθησης των λειτουργιών του συστήματος
- Την ευθύνη καθορισμού των Ιδιοκτητών Συστημάτων και των Διαχειριστών Συστημάτων την έχει η διοίκηση της VLP HELLAS SA.

Ο κύκλος ζωής των πληροφοριακών συστημάτων (ανάπτυξη/ απόκτηση, λειτουργία και συντήρηση) θα πρέπει να ακολουθεί την Πολιτική Ασφάλειας Πληροφοριών του Οργανισμού, και τις διεθνώς αναγνωρισμένες πρακτικές και πρότυπα ασφάλειας, ανεξάρτητα εάν η ανάπτυξη και συντήρηση αυτή πραγματοποιείται από το προσωπικό της VLP HELLAS SA ή από κατάλληλους εξωτερικούς συνεργάτες.

Ανάπτυξη/ Απόκτηση Πληροφοριακών Συστημάτων

Η ανάπτυξη νέων πληροφοριακών συστημάτων θα πρέπει να πραγματοποιείται σύμφωνα με τη χρήση αποδεκτών μεθοδολογιών και εργαλείων, και πρέπει να λαμβάνονται υπόψη και τα σχετικά με την ασφάλεια θέματα.

Κατά την ανάθεση ανάπτυξης του πληροφοριακού συστήματος σε εξωτερικό συνεργάτη, η σύμβαση πρέπει να διασφαλίζει τον Οργανισμό από πιθανή ζημία, η οποία πιθανόν να προκύψει από μη πλήρη συμφωνία του νέου συστήματος με τις προδιαγραφές που έχει ορίσει ο Οργανισμός. Επίσης, πρέπει να εξασφαλίζεται η σωστή υποστήριξη των συστημάτων από το τρίτο μέρος ανάλογα με τις απαιτήσεις ασφάλειας κάθε συστήματος και τις γενικότερες επιχειρησιακές απαιτήσεις.

Σε κάθε περίπτωση, πριν τεθεί το νέο πληροφοριακό σύστημα σε λειτουργία, πρέπει να προηγούνται αναλυτικοί έλεγχοι που να επιβεβαιώνουν την ικανοποίηση των απαιτήσεων ασφάλειας.

Τα πληροφοριακά συστήματα της VLP HELLAS SA θα πρέπει να ταξινομούνται σύμφωνα με το υπάρχον Σχήμα Διαβάθμισης Πληροφοριών. Οι ακόλουθοι παράγοντες πρέπει να λαμβάνονται υπόψη:

- Η κρισιμότητα των δεδομένων που επεξεργάζονται
- Η αλληλεξάρτηση με άλλα κρίσιμα πληροφοριακά συστήματα

Λειτουργία και Συντήρηση Πληροφοριακών Συστημάτων

Όλα τα πληροφοριακά συστήματα πρέπει να εποπτεύονται επαρκώς ανάλογα με την κρισιμότητά τους, και να συντηρούνται ανάλογα με τις συστάσεις των κατασκευαστών και τις προδιαγραφές τους, ώστε να εξασφαλίζεται η σωστή και απρόσκοπτη λειτουργία τους καθώς και η έγκαιρη διάγνωση βλαβών και αποκατάστασή τους.

Όλες οι δραστηριότητες που αφορούν στη λειτουργία των πληροφοριακών συστημάτων πρέπει να γίνονται βάσει εγκεκριμένων διαδικασιών και μόνο από το αρμόδιο προσωπικό του Οργανισμού.

Αρχεία Καταγραφής

Όλα τα συστήματα πρέπει να έχουν ενεργοποιημένες τις δυνατότητες καταγραφής συμβάντων σε αρχεία (logs), ειδικά στη περίπτωση που αφορούν την ασφάλεια. Τα στοιχεία που πρέπει να περιλαμβάνουν τα αρχεία καταγραφής εξαρτώνται τόσο από την κρισιμότητα όσο και από τις τεχνικές δυνατότητες του συστήματος.

Ο Οργανισμός ορίζει το χρονικό διάστημα τήρησης των αρχείων καταγραφής των πληροφοριακών συστημάτων, λαμβάνοντας υπόψη απαιτήσεις ασφάλειας καθώς και

τυχόν νομικές υποχρεώσεις.

Τροποποίηση Λειτουργίας (Change & Patch Management)

Όλες οι αλλαγές στην παραμετροποίηση συστημάτων, είτε αυτές σχετίζονται με τροποποιήσεις στο υλικό, είτε με τροποποιήσεις στο λογισμικό, πρέπει να είναι καταγεγραμμένες και να συνοδεύονται από όλες τις σχετικές πληροφορίες (ποιος έκανε την αλλαγή, πότε, για ποιο λόγο, τι ακριβώς αλλαγή έγινε κλπ).

Πριν από οποιαδήποτε αλλαγή σε πληροφοριακό σύστημα πρέπει να ενημερώνονται όλοι οι χρήστες των οποίων η εργασία πρόκειται να επηρεαστεί.

Απόσυρση Πληροφοριακών Συστημάτων

Η απόσυρση των πληροφοριακών συστημάτων του Οργανισμού πραγματοποιείται μόνο όταν δεν απαιτείται πλέον η χρήση τους και δεν υπάρχει καμία άλλου είδους απαίτηση επαναφοράς των αρχείων που έχουν δημιουργηθεί από αυτά (π.χ. νομική, επιχειρηματική κλπ.). Για το σκοπό αυτό, οι Ιδιοκτήτες Συστημάτων θα πρέπει να επανεξετάζουν την αξία και τη χρησιμότητα των πληροφοριακών συστημάτων ανά τακτά χρονικά διαστήματα.

Όλα τα πληροφοριακά συστήματα αλλά και τα αποθηκευτικά μέσα που παύουν να εξυπηρετούν τις ανάγκες του Οργανισμού θα πρέπει να καταστρέφονται με ασφαλή τρόπο και να ακολουθούν τη Διαδικασία Απόκτησης/ Ανάπτυξης και Απόσυρσης Πληροφοριακών Συστημάτων.

8.12 .Διενέργεια Ελέγχων Ασφάλειας

Η VLP HELLAS SA πρέπει να αναπτύσσει και να ακολουθεί ένα πλάνο συστηματικού ελέγχου της ασφάλειας τόσο σε οργανωτικό όσο και σε τεχνικό επίπεδο. Σκοπός είναι να μπορεί να διαπιστώσει την αποτελεσματικότητα των υπαρχόντων μηχανισμών ασφάλειας και της εφαρμογής της πολιτικής και των διαδικασιών ασφάλειας και να εντοπίσει πιθανές αδυναμίες.

Οι έλεγχοι ασφάλειας πρέπει να διενεργούνται από εξουσιοδοτημένα άτομα και το προσωπικό οφείλει να συνεργάζεται κατά τη διεξαγωγή των ελέγχων.

8.13 .Διαχείριση Λογικής Πρόσβασης

Πρόσβαση στους πόρους της VLP HELLAS SA (συστήματα, δίκτυο, πληροφορίες) πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα και μόνο στο πλαίσιο της διεκπεραίωσης των καθηκόντων τους.

Το επίπεδο «λογικής πρόσβασης» πρέπει να είναι ανάλογο με τις απαιτήσεις ασφάλειας της πληροφορίας και του πληροφοριακού συστήματος και να προσδιορίζεται από την επιχειρηματική ανάγκη για τη διεκπεραίωση επαγγελματικών καθηκόντων.

Τα θέματα αναφορικά με τη διαχείριση της λογικής πρόσβασης των χρηστών περιγράφονται παρακάτω.

Πεδίο Εφαρμογής

Η παρούσα πολιτική απευθύνεται σε όλους τους υπαλλήλους και τους εξωτερικούς της VLP HELLAS SA, οι οποίοι χρειάζονται πρόσβαση στα πληροφοριακά συστήματα του Οργανισμού για την εκπλήρωση των εργασιακών καθηκόντων τους.

Γενικές Αρχές

Δικαιώματα & Μηχανισμοί Πρόσβασης Χρηστών

Τα δικαιώματα πρόσβασης που δύναται να αποκτήσει ο κάθε χρήστης στα συστήματα του Οργανισμού πρέπει να είναι επακριβώς ορισμένα και αυστηρά συνδεδεμένα με τις απαιτήσεις της εργασίας του, βάσει του ρόλου του στην ομάδα στην οποία ανήκει.

Τα δικαιώματα πρόσβασης πρέπει να παραχωρούνται βάσει της ανάγκης γνώσης (“Need- to-know”) για την αποφυγή θεμιτής ή αθέμιτης αποκάλυψης πληροφοριών. Συνεπώς, πρέπει να παρέχεται μόνο το ελάχιστο αποδεκτό επίπεδο προνομίων στους χρήστες έτσι ώστε να μπορούν να εκτελούν τις καθημερινές εργασίες τους.

Κάθε χρήστης είναι συνδεδεμένος με ένα μοναδικό αναγνωριστικό (user id) και συνθηματικό, ως μέσο ταυτοποίησης και αυθεντικοποίησης στα συστήματα του Οργανισμού. Κάθε χρήστης φέρει αποκλειστική ευθύνη για οποιαδήποτε ενέργεια λαμβάνει χώρα μέσω του προσωπικού του λογαριασμού (user id/ password).

Η χρήση ομαδικών λογαριασμών (Group accounts) πρέπει να αποφεύγεται, εκτός εάν υπάρχει συγκεκριμένη επιχειρησιακή ανάγκη. Σε μια τέτοια περίπτωση πρέπει να υπάρχει έγκριση από τη διοίκηση της VLP HELLAS SA και τον Υπεύθυνο Ασφαλείας.

Στη περίπτωση που η πρόσβαση σε δυο ή περισσότερες υπηρεσίες απαιτεί τη δημιουργία περαιτέρω λογαριασμών για ένα χρήστη, τότε οι λογαριασμοί αυτοί θα πρέπει να έχουν μεταξύ τους διαφορετικά συνθηματικά.

Η χορήγηση προνομιακών δικαιωμάτων πρόσβασης (privileged accounts) είναι επιτρεπτή μόνο όταν απαιτείται από το ρόλο του χρήστη (π.χ. διαχειριστής δικτύου). Για τη χορήγηση προνομιακών δικαιωμάτων είναι απαραίτητη η έγκριση του Ιδιοκτήτη Συστήματος και του Υπεύθυνου Ασφαλείας.

Τροποποίηση και Κατάργηση Δικαιωμάτων Πρόσβασης

Σε περίπτωση που κάποιος υπάλληλος αλλάξει ρόλο και αρμοδιότητες, ο αντίστοιχος προϊστάμενός του πρέπει να εγκρίνει τα νέα δικαιώματα πρόσβασης που αντιστοιχούν στα νέα του καθήκοντα. Κατά συνέπεια, τα δικαιώματα πρόσβασης που δεν χρειάζονται στη νέα θέση εργασίας του χρήστη, πρέπει να καταργούνται αμέσως.

Τα δικαιώματα πρόσβασης των χρηστών και των εξωτερικών της VLP HELLAS SA πρέπει να καταργούνται άμεσα μετά την αποχώρηση του χρήστη από τον Οργανισμό και τη λήξη του έργου αντίστοιχα. Σε περίπτωση που ο υπάλληλος που αποχωρεί γνωρίζει συνθηματικά λογαριασμών που χρειάζεται να παραμείνουν ενεργοί, τότε τα συνθηματικά των λογαριασμών πρέπει να αλλάζουν κατά τη λήξη της απασχόλησης του χρήστη.

8.14 .Χρήση Ηλεκτρονικού Ταχυδρομείου και Διαδικτύου

Η προσωπική χρήση του ηλεκτρονικού ταχυδρομείου και των υπηρεσιών του διαδικτύου οφείλει να γίνεται στο πλαίσιο των καθηκόντων του προσωπικού και των εργαζομένων της VLP HELLAS SA και δεν πρέπει σε καμία περίπτωση να παρεμβαίνει ή να έρχεται σε σύγκρουση με αυτά.

Η VLP HELLAS SA πρέπει να θέσει τους κανόνες για την σωστή και αποδεκτή χρήση του ηλεκτρονικού ταχυδρομείου και του διαδικτύου και να υλοποιήσει τα κατάλληλα μέτρα έτσι ώστε να προστατεύσει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των εταιρικών πληροφοριών και υποδομών.

Η VLP HELLAS SA οφείλει να ενημερώνει εγκαίρως τους χρήστες για τους επικείμενους κινδύνους και τις νομικές επιπτώσεις από την κατάχρηση του ηλεκτρονικού ταχυδρομείου και του διαδικτύου.

Τα θέματα αποδεκτής χρήσης του ηλεκτρονικού ταχυδρομείου και του διαδικτύου περιγράφονται παρακάτω:

Αποδεκτή Χρήση Ηλεκτρονικού Ταχυδρομείου και Διαδικτύου

Η χρήση του ηλεκτρονικού ταχυδρομείου και του διαδικτύου γίνεται στο πλαίσιο της διευκόλυνσης της διεξαγωγής των εργασιακών καθηκόντων (need-to-have basis) των χρηστών. Ενδεικτικά εξυπηρετεί την:

- Επικοινωνία μεταξύ των υπαλλήλων του Οργανισμού και των εξωτερικών συνεργατών στο πλαίσιο των εργασιακών αναγκών
- Μετάδοση των πληροφοριών, οι οποίες σχετίζονται με τις λειτουργίες του Οργανισμού
- Ενημέρωση των χρηστών στο πλαίσιο των εργασιακών τους καθηκόντων

Οι χρήστες πρέπει να είναι προσεκτικοί με τα ηλεκτρονικά μηνύματα από άγνωστους αποστολείς ή και με τη χρήση των επισυναπτόμενων αρχείων καθώς ενδέχεται να περιέχουν ιούς ή συνδέσεις (links) σε παράνομες ιστοσελίδες.

Μη Αποδεκτή Χρήση Ηλεκτρονικού Ταχυδρομείου και Διαδικτύου

Οι χρήστες θα πρέπει να αποφεύγουν την αποστολή ευαίσθητων πληροφοριών μέσω του ηλεκτρονικού ταχυδρομείου. Σε περίπτωση που υπάρχει επιχειρησιακή ανάγκη, οι πληροφορίες θα πρέπει να κρυπτογραφούνται.

Οι ακόλουθες ενέργειες δεν επιτρέπονται κατά τη χρήση του ηλεκτρονικού ταχυδρομείου:

- Αποστολή ηλεκτρονικών μηνυμάτων σε μεγάλο αριθμό χρηστών, εκτός αν υπάρχει συγκεκριμένη επιχειρησιακή ανάγκη
- Αντιγραφή, καταστροφή ή αποδοχή και χρήση υλικού που προστατεύεται από δικαιώματα πνευματικής ιδιοκτησίας
- Αποστολή ιομορφικού λογισμικού
- Αποστολή ή αποδοχή προσβλητικού, ρατσιστικού ή άλλου παράνομου υλικού
- Προσπάθεια μη εξουσιοδοτημένης πρόσβασης στους λογαριασμούς ηλεκτρονικού ταχυδρομείου άλλων χρηστών
- Κάθε παράνομη δραστηριότητα
- Οι ακόλουθες ενέργειες δεν επιτρέπονται κατά τη χρήση του διαδικτύου:
- Συμμετοχή σε παιχνίδια, δημοπρασίες, ομάδες ανοιχτών συζητήσεων (chat rooms)

- για μη επιχειρησιακούς σκοπούς
- Οποιαδήποτε ενέργεια ή προτροπή σε ενέργεια η οποία παραβιάζει το ισχύον νομικό και κανονιστικό πλαίσιο

8.15. Διαχείριση Περιστατικών Ασφάλειας

Η VLP HELLAS SA πρέπει να έχει λάβει όλα τα απαραίτητα οργανωτικά και τεχνολογικά μέτρα για την πρόληψη και την αντιμετώπιση των περιστατικών ασφάλειας, με σκοπό να είναι δυνατός ο έγκαιρος χειρισμός τους πριν πραγματοποιηθεί σημαντική ζημιά. Όλα τα ύποπτα περιστατικά πρέπει να διερευνώνται από το αρμόδιο προσωπικό, σύμφωνα με τις καταγεγραμμένες διαδικασίες.

Η VLP HELLAS SA πρέπει να αναπτύξει τους κατάλληλους διαύλους επικοινωνίας για την αναφορά των περιστατικών ασφάλειας και να τους γνωστοποιήσει σε όλο το προσωπικό του.

Τα θέματα διαχείρισης περιστατικών ασφάλειας περιγράφονται παρακάτω.

Πεδίο Εφαρμογής

Η παρούσα πολιτική ασφάλειας αφορά σε όλα τα πληροφοριακά συστήματα που στηρίζουν τη λειτουργία της VLP HELLAS SA. Επίσης, αφορά όλους τους χρήστες και τους εξωτερικούς συνεργάτες που αποκτούν πρόσβαση σε αυτά και στις πληροφορίες της VLP HELLAS SA κατά τη διάρκεια της συνεργασίας τους με τον Οργανισμό.

Γενικές Αρχές

Γενικές Αρχές Διαχείρισης Περιστατικών Ασφάλειας

Η VLP HELLAS SA εφαρμόζει όλους τους απαραίτητους μηχανισμούς ασφαλείας για την προστασία των πληροφοριακών συστημάτων από ενδεχόμενα περιστατικά ασφάλειας.

Η VLP HELLAS SA πρέπει να ορίσει με σαφήνεια τους απαραίτητους ρόλους και τις αντίστοιχες αρμοδιότητες για την άμεση και ορθή αντιμετώπιση των ενδεχόμενων περιστατικών ασφάλειας. Οι ρόλοι πρέπει να ανατεθούν σε κατάλληλα καταρτισμένους υπαλλήλους του Οργανισμού ή εξωτερικούς συνεργάτες.

Οι χρήστες δεν επιτρέπεται να αποκαλύπτουν πληροφορίες που σχετίζονται με τα περιστατικά ασφάλειας. Οι πληροφορίες αυτές συζητούνται μόνο με το υπεύθυνο και εξουσιοδοτημένο προσωπικό της VLP HELLAS SA.

Η VLP HELLAS SA έχει ορίσει τον Υπεύθυνο Ασφάλειας ως το σημείο επικοινωνίας και αναφοράς των περιστατικών ασφάλειας.

Κάθε μορφή παρεμπόδισης του προσωπικού να εκτελέσει το έργο του κατά το στάδιο της αναφοράς, της έρευνας και της αντιμετώπισης των περιστατικών ασφάλειας, θεωρείται μη συμμόρφωση με τη Πολιτική Ασφάλειας Πληροφοριών και ενδέχεται να υπάρξουν πειθαρχικές κυρώσεις.

Ο Υπεύθυνος Ασφάλειας είναι υπεύθυνος να αξιολογήσει εάν το περιστατικό ασφάλειας οφείλεται σε κακόβουλες ενέργειες που προέρχονται από τους

εσωτερικούς χρήστες της VLP HELLAS SA είτε από εξωτερικούς παράγοντες και ανάλογα να ενημερώσει άμεσα τη Διοίκηση, ώστε να καθοριστούν οι ενέργειες για την αντιμετώπισή του.

Για την αντιμετώπιση των περιστατικών ασφάλειας, ο Υπεύθυνος Ασφάλειας και η Διοίκηση της VLP HELLAS SA είναι αρμόδιοι να συστήσουν την «Ομάδα Χειρισμού Περιστατικών Ασφάλειας». Η Ομάδα αποτελείται από κατάλληλα εκπαιδευμένο προσωπικό για την επιτυχή αντιμετώπιση του περιστατικού ασφάλειας. Η σύνθεση της Ομάδας Χειρισμού Περιστατικών Ασφάλειας διαμορφώνεται ανάλογα με τη σοβαρότητα και τον τύπο του περιστατικού ασφάλειας.

Η Ομάδα Χειρισμού Περιστατικών Ασφάλειας μαζί με τη Διοίκηση της VLP HELLAS SA είναι αρμόδια να εξετάσει εάν απαιτείται ή χρειάζεται η συμβολή εξωτερικών συνεργατών για την αντιμετώπιση του περιστατικού ασφάλειας. Σε μια τέτοια περίπτωση, οι εξωτερικοί συνεργάτες θα πρέπει να λάβουν γνώση και να αποδεχτούν τις σχετικές αρμοδιότητες και ευθύνες τους όπως αυτές ορίζονται στην Πολιτική Ασφάλειας για τις σχέσεις με εξωτερικούς συνεργάτες.

Κάθε περιστατικό ασφάλειας που επιβεβαιώνεται πρέπει να αξιολογείται ως προς τη κρισιμότητά του βάσει των δεδομένων ή πιθανών επιπτώσεων στον Οργανισμό. Η αξιολόγηση γίνεται από την Ομάδα Χειρισμού Περιστατικών Ασφάλειας. Ενδεικτικά:

- Υψηλή Προτεραιότητα: όταν έχουν διακυβευτεί ή είναι πολύ πιθανό να διακυβευτούν κρίσιμα πληροφοριακά συστήματα του Οργανισμού, με αποτέλεσμα να επηρεαστεί η ομαλή συνέχεια της λειτουργίας του και να υπάρξουν μεγάλες οικονομικές απώλειες.

- Μεσαία Προτεραιότητα: όταν υπάρχουν βάσιμες ενδείξεις ότι κρίσιμα ή/και υποστηρικτικά συστήματα του Οργανισμού είναι στόχος επίθεσης (π.χ. επιθέσεις τύπου denial of service, σημαντικός αριθμός scans σε πληροφοριακά συστήματα του Οργανισμού, διαρροή συνθηματικών προνομιούχων χρηστών)

- Χαμηλή Προτεραιότητα: όταν δεν υπάρχει άμεσος κίνδυνος, αλλά έχουν εντοπιστεί σημάδια επιθέσεων και παραβίασης στα πληροφοριακά συστήματα (π.χ. μικρός αριθμός αποτυχημένων προσπαθειών μη εξουσιοδοτημένης πρόσβασης σε πληροφοριακά συστήματα).

Μετά την αντιμετώπιση του περιστατικού διεξάγεται ανάλογη έρευνα με στόχο την ανακάλυψη των αιτιών της πραγματοποίησης του περιστατικού ασφάλειας και τις άμεσες και έμμεσες επιπτώσεις του περιστατικού ασφάλειας. Επιπρόσθετα, γίνεται αξιολόγηση των ενεργειών που έλαβαν χώρα. Ο Υπεύθυνος Ασφάλειας πρέπει να τηρεί ενημερωμένο αρχείο που θα περιέχει τις παραπάνω πληροφορίες καθώς μπορεί να χρησιμοποιηθούν κατά τη διεξαγωγή αποτίμησης κινδύνου και κατά την αξιολόγηση των υπαρχόντων μηχανισμών ασφάλειας των πληροφοριακών συστημάτων. Ο απώτερος σκοπός είναι η απόκτηση εμπειρίας από το περιστατικό ασφάλειας.

Μετά την αντιμετώπιση του περιστατικού ασφάλειας, πρέπει να διεξάγεται έλεγχος των μηχανισμών ασφάλειας στα πληροφοριακά συστήματα που είχαν επηρεαστεί. Ο έλεγχος μπορεί να πραγματοποιείται είτε από το προσωπικό, είτε από εξωτερικούς συνεργάτες, εάν αυτό κρίνεται απαραίτητο.

Υποχρεώσεις Προσωπικού

Όλοι οι υπάλληλοι της VLP HELLAS SA οφείλουν να είναι ενήμεροι με την παρούσα

πολιτική ασφάλειας και να τις εφαρμόζουν όταν παραστεί ανάγκη.

Όλοι οι υπάλληλοι της VLP HELLAS SA είναι υπεύθυνοι να παρατηρούν και να αναφέρουν κάθε ύποπτο περιστατικό ασφάλειας και κάθε πιθανή αδυναμία των πληροφοριακών συστημάτων στον Υπεύθυνο Ασφάλειας. Ιδιαίτερα οι διαχειριστές συστημάτων είναι υπεύθυνοι να παρατηρούν και να αναφέρουν οποιαδήποτε αδυναμία του πληροφοριακού συστήματος που θα υποπέσει στην αντίληψή τους κατά τη διεξαγωγή των εργασιακών τους καθηκόντων. Οι χρήστες δεν πρέπει να αποκαλύπτουν τις αντίστοιχες πληροφορίες σε μη εξουσιοδοτημένα άτομα, σε καμία περίπτωση.

Οι χρήστες δεν πρέπει σε καμία περίπτωση να επιχειρούν αυτόβουλη παρέμβαση στα πληροφοριακά συστήματα, εκτός εάν είναι εξουσιοδοτημένοι. Μόνο το εξειδικευμένα προσωπικό συμμετέχει στην ανάκαμψη των συστημάτων στη κανονική τους λειτουργία.

Προστασία από Κακόβουλο Λογισμικό

Η VLP HELLAS SA οφείλει να λαμβάνει όλα τα απαραίτητα οργανωτικά και τεχνικά μέτρα ασφάλειας, τα οποία αποσκοπούν στην αποτροπή, ανίχνευση και αντιμετώπιση του κακόβουλου λογισμικού.

Η VLP HELLAS SA οφείλει να ενημερώνει τους εργαζόμενους αναφορικά με τους κινδύνους από το κακόβουλο λογισμικό καθώς και για τις υποχρεώσεις τους σε σχέση με τα μέτρα προστασίας έναντι του κακόβουλου λογισμικού.

Η VLP HELLAS SA οφείλει, να πραγματοποιεί έλεγχο της ακεραιότητας του λογισμικού των ΠΕΣ. Ο έλεγχος αυτός έχει ως σκοπό τη διαπίστωση της μη ύπαρξης λογισμικού στα ΠΕΣ πέραν αυτού που έχει επισήμως προμηθευτεί.

8.16 .Διαχείριση Επιχειρησιακής Συνέχειας

8.16.1. Διαχείριση Αντιγράφων Ασφάλειας

Η VLP HELLAS SA πρέπει να έχει επίσημο και καταγεγραμμένο σχέδιο λήψης και ανάκτησης αντιγράφων ασφάλειας (backup) τόσο για το λογισμικό (software) όσο και για τα εταιρικά δεδομένα. Τα αντίγραφα ασφάλειας πρέπει να ελέγχονται για να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και διαθεσιμότητά τους. Η ποσότητα, η συχνότητα λήψης και η χρονική διάρκεια τήρησης των αντιγράφων ασφάλειας πρέπει να λαμβάνει υπόψη την κρισιμότητα των πληροφοριών και να είναι πλήρης και συνεχής.

Η λήψη και η ανάκτηση των αντιγράφων ασφάλειας πρέπει να είναι σύμφωνη με την Πολιτική Αντιγράφων Ασφάλειας.

Πεδίο Εφαρμογής

Η παρούσα πολιτική απευθύνεται σε όλα τα πληροφοριακά συστήματα που στηρίζουν τη λειτουργία του Οργανισμού. Επίσης, η πολιτική απευθύνεται στους Ιδιοκτήτες

Συστημάτων και στους Διαχειριστές Συστημάτων του Οργανισμού

Γενικές Αρχές

Δημιουργία Αντιγράφων Ασφάλειας

Η δημιουργία και η αποθήκευση των αντιγράφων ασφαλείας πρέπει να είναι σύμφωνη με τις καταγεγραμμένες διαδικασίες του Οργανισμού. Υπεύθυνος για τη δημιουργία των απαιτούμενων αντιγράφων ασφαλείας είναι ο εκάστοτε Διαχειριστής Συστήματος.

Τα μέσα αντιγράφων ασφαλείας πρέπει να αναγράφουν ευκρινώς την ονομασία του συστήματος και την ημερομηνία δημιουργίας τους.

Ο Οργανισμός λαμβάνει όλα τα απαραίτητα μέτρα για τη προστασία των μέσων αποθήκευσης των αντιγράφων ασφαλείας, έτσι ώστε τα περιεχόμενά τους να μην αλλοιωθούν ή καταστραφούν κατά λάθος.

Τα αντίγραφα ασφαλείας έχουν τον ίδιο βαθμό διαβάθμισης με τις πληροφορίες που περιέχουν. Ο Οργανισμός εξετάζει εάν υπάρχει ανάγκη να χρησιμοποιηθεί κρυπτογράφηση των υψηλά διαβαθμισμένων πληροφοριών των αντιγράφων ασφαλείας.

Σε περίπτωση που προκύψει πρόβλημα κατά τη διάρκεια λήψης αντιγράφων ασφαλείας, πρέπει να ενημερωθεί άμεσα ο Ιδιοκτήτης Συστήματος.

Αρχές Διαχείρισης Αντιγράφων Ασφαλείας

Οι απαιτήσεις αναφορικά με τον τύπο, τη συχνότητα λήψης και την αποθήκευση των αντιγράφων ασφαλείας πρέπει να καθορίζονται από το βαθμό κρισιμότητας των πληροφοριών και τις επιχειρηματικές ανάγκες του Οργανισμού.

Στα αντίγραφα ασφαλείας πρέπει να παρέχεται ανάλογο επίπεδο προστασίας με τα αρχικά στοιχεία και να παρέχονται αντίστοιχα μέτρα ασφάλειας. Η διαχείριση των αντιγράφων ασφαλείας πρέπει να είναι σύμφωνη με τις αρχές της Πολιτικής Διαχείρισης Αποθηκευτικών Μέσων και Εγγράφων.

Τα αντίγραφα ασφαλείας πρέπει να αποθηκεύονται σε ασφαλές περιβάλλον (π.χ. ντουλάπια με κλειδιά, χρηματοκιβώτιο). Τα αντίγραφα ασφάλειας θα πρέπει να φυλάσσονται για όσο χρόνο είναι απαραίτητο και όχι για περισσότερο.

Η πρόσβαση στα αντίγραφα ασφαλείας πρέπει να περιορίζεται στο εξουσιοδοτημένο προσωπικό του Οργανισμού λαμβάνοντας υπόψη τις αρχές της Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας.

Ο Οργανισμός για τα αντίγραφα ασφάλειας που αφορούν κρίσιμα πληροφοριακά συστήματα, πρέπει να διατηρεί δύο διαφορετικά σετ αντιγράφων ασφαλείας, τα οποία πρέπει να αποθηκεύονται σε διαφορετικούς χώρους.

Ανάκαμψη Συστημάτων

Η ανάκτηση των δεδομένων από τα αντίγραφα ασφαλείας πρέπει να είναι σύμφωνη με τη Διαδικασία Αντιγράφων Ασφαλείας.

Η αποτελεσματικότητα των διαδικασιών ανάκτησης των πληροφοριακών συστημάτων πρέπει να ελέγχεται ανά τακτά χρονικά διαστήματα. Σκοπός είναι να

εξασφαλιστεί η αποτελεσματικότητα της διαδικασίας αλλά και να εξοικειωθεί το αρμόδιο προσωπικό του Οργανισμού.

8.16.2. Πλάνο Επιχειρησιακής Συνέχειας

Η VLP HELLAS SA πρέπει να αναπτύξει και να τεκμηριώσει ένα συγκεκριμένο πλάνο για τη διαχείριση της επιχειρησιακής συνέχειας σε περίπτωση καταστροφικών συμβάντων που έχουν ως αποτέλεσμα τη διακοπή των κρίσιμων λειτουργιών της (φυσικών καταστροφών, αστοχία υλικού / λογισμικού, κακόβουλες ενέργειες κ.ά.). Σκοπός είναι η μείωση των αρνητικών επιπτώσεων στο επίπεδο που ορίζει η VLP HELLAS SA.

Το πλάνο επιχειρησιακής συνέχειας πρέπει να γνωστοποιείται στο αρμόδιο προσωπικό και να δοκιμάζεται έτσι ώστε σε περίπτωση καταστροφής να είναι αποτελεσματικό (E_06- Business Continuity Plan).

8.17 .Συμμόρφωση με την Ισχύουσα Νομοθεσία

Η VLP HELLAS SA οφείλει να παρακολουθεί συνεχώς και να συμμορφώνεται με το υφιστάμενο νομικό και κανονιστικό πλαίσιο όσον αφορά στην ασφάλεια των πληροφοριών. Ενδεικτικά, πρέπει να λαμβάνονται υπόψη οι νόμοι και οι ρυθμίσεις που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα, τη διασφάλιση του απορρήτου των επικοινωνιών, τα θέματα πνευματικής ιδιοκτησίας κ.ά.

9. Διαδικασίες - Φόρμες – Αρχεία

Τίτλος	Τοποθεσία	Χρόνος Τήρησης	Υπεύθυνος Τήρησης
Ε_07 Σχήμα Διαβάθμισης Πληροφοριών			
Α_03 Αρχείο Καταγραφής Εταιρικών Πόρων- Asset Registry			
Α_05 Αρχείο Καταστροφής Διαβαθμισμένων Εγγράφων & Αποθηκευτικών Μέσων			
Ε_04 Βεβαίωση Εμπιστευτικότητας			
Φ_03 Φορμα Αίτησης Ψηφιακού Ελέγχου			
Ε_06 Business Continuity Plan			