Πολιτική Ασφάλειας της Allweb Solutions S.A.

ΕΚΔΟΣΗ ΚΑΙ ΔΙΑΝΟΜΗ

• Α/Α ΕΚΔΟΣΗΣ ΕΓΧΕΙΡΙΔΙΟΥ	**2η**	
• ΕΚΔΟΣΗ ΕΓΧΕΙΡΙΔΙΟΥ ΑΠΟ	**ΥΠΕΥΘΥΝΟ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ**	
• ΗΜΕΡΟΜΗΝΙΑ	**15-10-2020**	
• ΚΑΤΑΣΤΑΣΗ ΑΝΤΙΓΡΑΦΟΥ	• **ΕΛΕΓΧΟΜΕΝΟ**	**Χ**
	• **ΜΗ ΕΛΕΓΧΟΜΕΝΟ**	

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

Η Πολιτική Ασφάλειας περιγράφει το σύνολο των κανόνων που καθορίζουν τον τρόπο με τον οποίο η Allweb Solutions S.A. πρέπει να διαχειρίζεται και να προστατεύει τα Πληροφοριακά της Σύστημα, έτσι ώστε να επιτυγχάνει συγκεκριμένους στόχους ασφάλειας. Παρέχοντας καθοδήγηση στα στελέχη της Εταιρείας αναφορικά με τον τρόπο οργάνωσης και επεξεργασίας των πληροφοριών, η Πολιτική Ασφάλειας αποτελεί το πλέον αποτελεσματικό μέσο για την προστασία των δεδομένων που διαχειρίζεται η Allweb Solutions S.A..

Η Πολιτική Ασφάλειας δεν είναι απόλυτη ή στατική. Αντιθέτως, είναι ένα κείμενο με δυναμική που πρέπει να αντανακλά τις αλλαγές στις προτεραιότητες της Διοίκησης της Εταιρείας καθώς και τις αλλαγές στο περιβάλλον και τις τεχνολογικές εξελίξεις. Η δυναμική αυτή επιβάλλει την συνεχή αναθεώρησή της ώστε να είναι πάντα επίκαιρη, σύμφωνα με τις εκάστοτε συνθήκες.

Η Πολιτική Ασφάλειας βασίστηκε στις απαιτήσεις των στρατηγικών κατευθύνσεων της Εταιρείας, σε σχέση με την αξιοποίηση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) και την ασφάλειά τους.

2. ΑΡΧΕΣ ΔΙΑΜΟΡΦΩΣΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Η Πολιτική Ασφάλειας του Πληροφοριακού Συστήματος της Εταιρείας Allweb Solutions S.A. δείχνει την πρόθεση της διοίκησης της Εταιρείας να προστατέψει τα Πληροφοριακά Σύστηματα. Με τη βοήθεια της Πολιτικής Ασφάλειας, η Εταιρεία Allweb Solutions S.A. καλείται να επιτύχει τους ακόλουθους στόχους:

- Συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο που αφορά την προστασία προσωπικών δεδομένων και τη διασφάλιση του απορρήτου των επικοινωνιών
- Διασφάλιση της επιχειρησιακής της ικανότητας, στο βαθμό που εξαρτάται από την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα πληροφοριών και επικοινωνιών.

Λαμβάνοντας υπόψη τους στόχους προς επίτευξη, κατά την ανάπτυξη και σύνταξη της Πολιτικής Ασφάλειας που αφορά τα Πληροφοριακά Σύστηματα της Allweb Solutions S.A., η Πολιτική Ασφάλειας έχει τα ακόλουθα χαρακτηριστικά:

- Είναι **επίκαιρη** σε σχέση με τις τρέχουσες τεχνολογικές εξελίξεις.
- Είναι **γενικεύσιμή**, ώστε η εφαρμογή της να είναι επεκτάσιμή σε μελλοντικές νέες δραστηριότητες της Allweb Solutions S.A.
- Είναι **σαφής**, ώστε να μην παρουσιάζονται δυσκολίες στην κατανόηση και εφαρμογή της.
- Αποτελεί πολιτική απαλλαγμένη από μη απαραίτητους τεχνικούς όρους, που θα την καθιστούσαν δύσκολη στην εφαρμογή και εξαρτημένη από τεχνολογικές επιλογές.

Η Πολιτική Ασφάλειας συντάχθηκε με γνώμονα ορισμένες βασικές αρχές, οι οποίες είναι οι ακόλουθες:

- Αποφυγή συγκεκριμένων ή εξειδικευμένων αναφορών έτσι ώστε να μην τροποποιείται συχνά, αλλά μόνον όταν συμβαίνουν σημαντικές αλλαγές στην διαχείριση της ασφάλειας του ΟΠΣ.
- Να είναι κατανοητή, αποτελεσματική και εφαρμόσιμή από άποψη κόστους.
- Να μην έχει τεχνικό μόνο χαρακτήρα.
- Να περιλαμβάνει ένα οργανωτικό πλαίσιο ρόλων και αρμοδιοτήτων για την ορθή εφαρμογή της.Για την πληρέστερη αξιοποίηση της Πολιτικής Ασφάλειας, το περιεχόμενό της θα πρέπει να γίνει γνωστό σε κάθε εργαζόμενο που εμπλέκεται στη χρήση του Πληροφοριακού Συστήματος. Αυτό απαιτεί την εκπαίδευση των εργαζομένων στη εφαρμογή της Πολιτικής Ασφάλειας.

3. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η διαδικασία αυτή εφαρμόζεται σε όλα τα Έγγραφα του ΣΔΑΠ, δηλαδή:

- Τις Πολιτικές Ασφάλειας
- Το Πεδίο Εφαρμογής του Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών
- Στις Διαδικασίες Διαχείρισης της Ασφάλειας.
- Στις Οδηγίες Εργασίας (Προδιαγραφές, Οδηγίες Επιθεωρήσεων, Οδηγίες Συντήρησης Εξοπλισμού, κ.λ.π).
- Σε άλλα Έγγραφα Εσωτερικής ή Εξωτερικής Προέλευσης, τα οποία επηρεάζουν άμεσα ή έμμεσα την ασφάλεια των πληροφοριών που η επιχείρηση διαχειρίζεται.

4. ΟΡΙΣΜΟΙ - ΣΥΝΤΜΗΣΕΙΣ

ΥΔΑΠ Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών
ΥΠΣ Υπεύθυνος Πληροφοριακών Συστημάτων
ΣΔΑΠ Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών

5. ΕΦΑΡΜΟΓΗ

5.1 ΕΝΕΡΓΕΙΕΣ

- Στα πλαίσια των ανωτέρω η Διοίκηση εφαρμόζει τη παρούσα Πολιτική σε όλο το εύρος του Οργανισμού. Η εφαρμογή της και η αποτελεσματικότητα επίσης ελέγχονται. Η ενημέρωση του προσωπικού αξιολογείται τακτικά. Τα συμβάντα ασφάλειας αναγνωρίζονται έγκαιρα και λαμβάνονται αντίστοιχες διορθωτικές ενέργειες.
- Οι αδυναμίες του περιβάλλοντος του οργανισμού αξιολογούνται τακτικά.
- Τα συστήματα πληροφορικής και επικοινωνιών της εταιρείας ελέγχονται για να είναι πάντα στις τελευταίες ενημερωμένες εκδόσεις λογισμικού.
- Το προσωπικό από τη φύση του Οργανισμού είναι ενημερωμένο και έχει επαρκείς δεξιότητες σε θέματα Η/Υ. Η διοίκηση όμως αναγνωρίζοντας ότι συμβάντα ασφάλειας μπορεί να οφείλονται σε μη ενημέρωση έχει εκπονήσει πρόγραμμα εκπαίδευσης για την αύξηση της εγρήγορσης του προσωπικού.
- Έχει αναπτυχθεί και εφαρμοστεί Πολιτική που απαιτεί ισχυρά passwords για όλους τους χρήστες. (βλ. Πολιτική Κωδικών – διαδικασία)
- Η επίδοση των συστημάτων παρακολουθείται συνεχώς.
- Τα logs που δημιουργούνται σε λειτουργικά συστήματα, εφαρμογές και συστήματα δικτύου ελέγχονται τακτικά.
- Οι διαδικασίες back-up & restore επανελέγχονται σε τακτά χρονικά διαστήματα..
- Έχει δημιουργηθεί μηχανισμός «ανταπόκρισης σε συμβάντα ασφάλειας» με σαφή καθήκοντα και διαδικασίες

5.2 ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η Πολιτική Ασφάλειας αποτελεί ακρογωνιαίο λίθο του Συστήματος Ασφάλειας Πληροφοριών. Ως εκ τούτου δεν προβλέπεται η συχνή αλλαγή της. Όμως επειδή το περιβάλλον αλλάζει με γοργούς ρυθμούς, σε τακτά χρονικά διαστήματα η Πολιτική θα ανασκοπείται για τη συνεχιζόμενη καταλληλότητά της και θα τροποποιείται αντίστοιχα αν απαιτείται.

6. ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

Ακολουθούν αναλυτικές πολιτικές Ασφαλείας ανά θεματική ενότητα.

I. ΓΕΝΙΚΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

1.0 Εισαγωγή

Με την πολιτική αυτή η διοίκηση της Allweb Solutions S.A. εκφράζει τη βούλησή της για τη διασφάλιση των Ολοκληρωμένων Πληροφοριακών Συστημάτων (ΟΠΣ) που υποστηρίζουν τις δραστηριότητες της εταιρείας και παρέχει τις βασικές κατευθύνσεις για τη διαχείριση της ασφάλειας των ΟΠΣ.

2.0 Σκοπός

Σκοπός της Πολιτικής διαχείρισης Ασφάλειας ΟΠΣ, είναι:

- Να εκφράσει ρητά τη βούληση της Allweb Solutions S.A. να διασφαλίσει τη λειτουργία των ΟΠΣ που υποστηρίζουν τις δραστηριότητές της.
- Να δώσει κατευθυντήριες οδηγίες στα στελέχη της Εταιρείας για τον τρόπο με τον οποίο πρέπει να αντιμετωπίζουν τα ζητήματα ασφάλειας ΟΠΣ.
- Να προδιαγράψει ένα Σύστημα διαχείρισης της Ασφάλειας των ΟΠΣ.

3.0 Πεδίο εφαρμογής

Η Πολιτική καλύπτει όλα τα ΟΠΣ που υποστηρίζουν δραστηριότητες της Allweb Solutions S.A. Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μμέρος της Πολιτικής Ασφάλειας ΟΠΣ.
Η Πολιτική απευθύνεται στα στελέχη της Allweb Solutions S.A.. που ασκούν διοικητικά καθήκοντα που σχετίζονται με τις δραστηριότητες της Allweb Solutions S.A. ή εποπτεύουν αυτές τις δραστηριότητες ή ασκούν διοίκηση σε τομείς που υποστηρίζουν τη λειτουργία των ΟΠΣ. Απευθύνεται, επίσης, στο σύνολο του προσωπικού που υποστηρίζει τη λειτουργία των ΟΠΣ καθώς και στους χρήστες, συνδρομητές, εργαζόμενους και συνεργάτες.

4.0 Πολιτική

4.1 Γενικές Αρχές

- **Βούληση της διοίκησης**
  - Η Εταιρεία αποδίδει υψηλή προτεραιότητα στην ασφάλεια των ΟΠΣ που υποστηρίζουν τις δραστηριότητές της.

- **Πολιτική ασφάλειας ΟΠΣ**
  - Η Allweb Solutions S.A. θεσπίζει και θέτει σε ισχύ την "Πολιτική Ασφάλειας ΟΠΣ". Η Πολιτική Ασφάλειας ΟΠΣ. αποτελείται από την παρούσα Πολιτική Ασφάλειας για τη διασφάλιση του Απορρήτου των Επικοινωνιών, καθώς και από ένα σύνολο θεματικών Πολιτικών Ασφάλειας.
- **Υποστήριξη εφαρμογής της Πολιτικής Ασφάλειας ΟΠΣ**
  - Η διοίκηση της Εταιρείας υποστηρίζει την εφαρμογή της Πολιτικής Ασφάλειας ΟΠΣ εξασφαλίζοντας τους απαραίτητους για αυτό το σκοπό πόρους και μέσα.
- **Διοικητική και οργανωτική υποστήριξη διαχείρισης της ασφάλειας ΟΠΣ**

- Με στόχο την αποτελεσματικότερη εφαρμογή της Πολιτικής Ασφάλειας ΟΠΣ, αναπτύσσεται η κατάλληλη διοικητική δομή, ορίζονται οι ρόλοι που είναι απαραίτητοι για τη διαχείρισης της ασφάλειας ΟΠΣ., καθορίζονται οι αρμοδιότητες για κάθε ρόλο και ανατίθενται οι ρόλοι στα κατάλληλα άτομα.

➢ **Συμμόρφωση με νομικό πλαίσιο**

- Η Διοίκηση και τα στελέχη της Εταιρείας προβαίνουν σε όλες τις ενέργειες που απαιτούνται για να γίνεται σεβαστή η νομοθεσία που αφορά την προστασία προσωπικών δεδομένων, το απόρρητο των επικοινωνιών, τα πνευματικά δικαιώματα, το ηλεκτρονικό έγκλημα και γενικά η νομοθεσία που αφορά τη χρήση ΟΠΣ.

4.1 Οδηγίες & κανόνες ασφάλειας

4.1.1 Πολιτική Ασφάλειας ΟΠΣ

- Η Πολιτική Ασφάλειας ΟΠΣ μπορεί να είναι έγγραφη ή/και ηλεκτρονική και να έχει επικυρωθεί από τη Διοίκηση της Εταιρείας. Η Πολιτική καλύπτει όλες τις κατηγορίες χρηστών (είτε είναι εταιρικοί χρήστες ή χρήστες υπηρεσιών που παρέχονται μέσω του διαδικτύου) που κάνουν χρήση των Πληροφοριακών Συστημάτων και των υπηρεσιών που παρέχονται.
- Η Εταιρεία προβαίνει σε όλες τις απαραίτητες ενέργειες, ώστε να ενημερώσει το προσωπικό για την Πολιτική Ασφάλειας ΟΠΣ και να εξασφαλίσει την άμεση και εύκολη πρόσβαση των υπαλλήλων στο πλήρες κείμενο της πολιτικής.
- Η Πολιτική Ασφάλειας των ΟΠΣ. της Εταιρείας συντάχθηκε με βάσει πέντε άξονες. Κάθε άξονας αντιπροσωπεύει ένα σύνολο επί μέρους πολιτικών που αφορούν συγκεκριμένους τομείς ασφάλειας. Οι βασικοί άξονες ασφάλειας είναι οι εξής:
  - Οργάνωση και Διαχείριση της Ασφάλειας ΟΠΣ,
  - Ασφάλεια Προσωπικού,
  - Έλεγχος Πρόσβασης,
  - Πρακτικές Θεμιτής Χρήσης, και
  - Ασφάλεια Ολοκληρωμένων Πληροφοριακών Συστημάτων.
- Η Πολιτική Ασφάλειας ΟΠΣ, καθορίζεται με βάση την επικινδυνότητα που ενέχεται στη λειτουργία των ΟΠΣ, όπως αυτή αποτιμάται με την ανάλυση επικινδυνότητας, η οποία πραγματοποιείται κατ' ελάχιστον κάθε δυο έτη και περιλαμβάνει τουλάχιστον τα παρακάτω :
  - Διατήρηση καταλόγου των ΣΠ με συνοπτική περιγραφή της λειτουργίας τους.
  - Αποτίμηση των απειλών που σχετίζονται με ενδεχόμενη παραβίαση του απορρήτου από εξωτερικές απειλές, εργαζόμενους ή συνεργάτες της εταιρείας, αποτίμηση των σχετικών ευπαθειών των ΟΠΣ και αποτίμηση των πιθανών επιπτώσεων των περιστατικών παραβίασης του απορρήτου.
- Η Πολιτική Ασφάλειας ΟΠΣ πρέπει να τυγχάνει τακτικής ανασκόπησης και να αναθεωρείται και επικαιροποιείται σε περίπτωση μείζονων αλλαγών στα ΟΠΣ της Allweb Solutions S.A., καθώς και σε περιπτώσεις σημαντικών μεταβολών του κοινωνικού και τεχνολογικού περιβάλλοντος, από τις οποίες προκύπτουν νέες απειλές, ευπάθειες, ή νέες ευκαιρίες βελτίωσης της ασφάλειας ΟΠΣ.
- Τα στελέχη της Εταιρείας πρέπει να συμβουλεύονται την Πολιτική ΟΠΣ, σε κάθε απόφασή τους, που αφορά ή μπορεί να επηρεάσει, άμεσα ή έμμεσα, την ασφάλεια των ΟΠΣ.
- Η εφαρμογή της Πολιτικής Ασφάλειας ΟΠΣ είναι υποχρεωτική. Η Εταιρεία λαμβάνει τα κατάλληλα μέτρα για την εφαρμογή της Πολιτικής Ασφάλειας ΟΠΣ.

4.1.2 Συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο

- Η Allweb Solutions S.A. δεσμεύεται για την τήρηση της νομοθεσίας που αφορά την προστασία προσωπικών δεδομένων, το απόρρητο των επικοινωνιών, τα πνευματικά δικαιώματα, το ηλεκτρονικό έγκλημα και γενικά τη νομοθεσία που αφορά τη χρήση ΟΠΣ, καθώς και για την εφαρμογή των σχετικών αποφάσεων της Αρχής Προστασίας Προσωπικών Δεδομένων και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών.
- Η Εταιρεία καταρτίζει και εφαρμόζει διαδικασίες που διασφαλίζουν τη διατήρηση των δεδομένων των επικοινωνιών για το χρονικό διάστημα που ορίζει η νομοθεσία.

- Η Εταιρεία προβαίνει σε όλες τις ενέργειες που απαιτούνται, ώστε να παρέχει στις Αρχές διευκολύνσεις και πληροφορίες, όπως προβλέπει η σχετική νομοθεσία. Η Εταιρεία διασφαλίζει ότι οι σχετικές διευκολύνσεις και πληροφορίες παρέχονται μόνο στις περιπτώσεις που προβλέπονται από τη νομοθεσία, ακολουθώντας νόμιμες διαδικασίες.
- Η Διοίκηση της Εταιρείας και ειδικότερα τα στελέχη της Διαχείρισης Ανθρώπινου Δυναμικού μεριμνούν ώστε όλα τα μέλη του προσωπικού να γνωρίζουν τις υποχρεώσεις τους που απορρέουν από τη νομοθεσία σχετικά με την επεξεργασία προσωπικών πληροφοριών και τη διασφάλιση του απορρήτου των επικοινωνιών.
- Η Διοίκηση μεριμνά για την ανάπτυξη οργανωτικών δομών και διαδικασιών με στόχο την προστασία της Εταιρείας από νομικές ενέργειες που στρέφονται εναντίον της.
- Η Εταιρεία μεριμνά για την προστασία του προσωπικού από νομικές συνέπειες που μπορεί να προκύψουν από ενέργειές τους στα πλαίσια της άσκησης των καθηκόντων τους και εφόσον τηρούν πιστά τις πολιτικές και τους κανονισμούς της Εταιρείας.

4.1.3 Οργανωτική υποδομή

- Η Εταιρεία αναπτύσσει κατάλληλες οργανωτικές και διοικητικές δομές για την αποτελεσματική διαχείριση της ασφάλειας ΟΠΣ. Η ευθύνη για τη διαχείριση της ασφάλειας ΟΠΣ ανατίθεται σε ανεξάρτητη Διεύθυνση. Ο επικεφαλής της Διεύθυνσης αναλαμβάνει το ρόλο του Υπεύθυνου Ασφάλειας ΟΠΣ.
- Η Εταιρεία μεριμνά για την επαρκή στελέχωση των στελεχών που έχουν ενεργό ρόλο στην ασφάλεια των ΟΠΣ.
- Στο οργανόγραμμά της Εταιρείας εντάσσεται ο ρόλος του Υπεύθυνου Ασφάλειας ΟΠΣ.
- Όλες οι διαδικασίες που αφορούν την ασφάλεια ΟΠΣ, είναι καταγεγραμμένες. Για κάθε διαδικασία πρέπει να ορίζεται ένας υπεύθυνος για την καταγραφή, τον έλεγχο της αποτελεσματικότητας, την επικαιροποίηση και τη διάθεσή της στα μέλη του προσωπικού που έχουν ανάγκη γνώσης ("need-to-know").

4.1.4 Έλεγχος Εφαρμογής Πολιτικής Ασφάλειας ΟΠΣ.

- Η εταιρεία οφείλει να διατηρεί Ειδικό Σχέδιο Αρχείων Καταγραφής, το οποίο, κατ' ελάχιστον, Περιλαμβάνει την αρχιτεκτονική και τις επιμέρους μεθόδους δημιουργίας, συλλογής, αποθήκευσης και διαχείρισης των αρχείων καταγραφής, πλήρη περιγραφή του περιεχομένου αυτών, καθώς και τα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς αυτών.
- Η εταιρεία οφείλει να εξασφαλίζει ότι οι καταγραφές που αναφέρονται στην Πολιτική Λογικής Πρόσβασης (παράγραφος 4.1 : αρχείο που καταγράφονται οι προσβάσεις των χρηστών των ΟΠΣ) καθώς και στην Πολιτική Διαχείρισης και Εγκατάστασης ΟΠΣ (παράγραφος 4.1) είναι πλήρεις και συνεχείς.
- Η εταιρεία οφείλει να ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, σύμφωνα με την αντίστοιχη πολιτική ασφάλειας , σε περίπτωση διακοπής των καταγραφών που προβλέπονται στα ως άνω άρθρα και σε περίπτωση περιστατικού παραβίασης της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας αυτών.
- Υπάρχουν κατάλληλα μέσα για την ανάλυση των αρχείων καταγραφής και την εξαγωγή σχετικών αναφορών.
- Τα αρχεία καταγραφής προστατεύονται με τρόπο που διασφαλίζει ότι ούτε οι διαχειριστές των ΟΠΣ έχουν τη δυνατότητα να προβούν σε ενέργειες που δεν καταγράφονται.
- Πραγματοποιούνται τακτικοί και έκτακτοι έλεγχοι.
- Οι έλεγχοι πραγματοποιούνται τόσο από το αρμόδιο τμήμα της Εταιρείας, όσο και από εξωτερικούς ελεγκτές.
- Ορίζεται διαδικασία καταγραφής και τεκμηρίωσης αδυναμιών συμμόρφωσης με τις απαιτήσεις που ορίζονται στην Πολιτική Ασφάλειας της εταιρείας, συμπεριλαμβανόμενων των επιμέρους πολιτικών και των διαδικασιών που την υλοποιούν.

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

II. ΠΟΛΙΤΙΚΗ ΕΓΓΡΑΦΩΝ, ΑΡΧΕΙΩΝ ΚΑΙ ΚΑΤΑΓΡΑΦΩΝ ΕΛΕΓΧΩΝ (Audit Trails/Logs/Records)

1.0 Εισαγωγή

Προκειμένου να εφαρμοστούν οι πολιτικές χρήσης πληροφοριών και τα μέτρα ασφάλειας, καθώς και για να είναι σε θέση η Εταιρεία να ερευνήσει τα περιστατικά ασφάλειας, πρέπει αυτοματοποιημένα να διατηρούνται αρχεία καταγραφής της πρόσβασης και των αλλαγών στα Πληροφοριακά Συστήματα και δεδομένα. Για να επιτευχθεί αυτό, πρέπει να διατηρείται ένα αρχείο της δραστηριότητας (ή "εγγραφών ελέγχου") των διεργασιών συστήματος και εφαρμογής καθώς και της δραστηριότητας των χρηστών Συστημάτων και εφαρμογών. Το αρχείο αυτό χρησιμοποιείται στη διερεύνηση των περιστατικών ασφάλειας, στον έλεγχο της χρήσης των πόρων της Εταιρείας, στην απόδοση ευθύνης για τις συναλλαγές, στην παρακολούθηση των αλλαγών στα συστήματα και στην παροχή βοήθειας για την ανίχνευση των ανωμαλιών συστήματος. Από κοινού με τα κατάλληλα εργαλεία και τις διαδικασίες, οι εγγραφές ελέγχου μπορούν να βοηθήσουν στην ανίχνευση των παραβιάσεων ασφάλειας, των προβλημάτων απόδοσης και των ελαττωμάτων στις εφαρμογές.

2.0 Σκοπός

Σκοπός της πολιτικής αυτής είναι η διατήρηση των εγγραφών ελέγχου με στόχο την απόδοση ευθύνης για τη χρήση των Ολοκληρωμένων Πληροφοριακών Συστημάτων (ΟΠΣ) της Εταιρείας.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλα τα πληροφοριακά συστήματα της Εταιρείας και για όλους τους χρήστες, διαχειριστές και υπεύθυνους Συστημάτων πληροφοριών.

4.0 Πολιτική

4.1 Διαδικασίες & Οδηγίες

a) Για τα ΟΠΣ της Εταιρείας διατηρούνται Εγγραφές Ελέγχου:

1) Κατ' ελάχιστο, οι ακόλουθες συναλλαγές πρέπει να καταγραφούν για κάθε Κεντρικό Υπολογιστή που βρισκεται στις υποδομές μας:

- Εκκίνηση και τερματισμός του κεντρικού υπολογιστή
- Load και unload των υπηρεσιών
- Εγκατάσταση και αφαίρεση λογισμικού
- Ειδοποιήσεις και μηνύματα λάθους συστήματος

- Σύνδεση και έξοδος των χρηστών από το σύστημα
- Δραστηριότητες διαχείρισης συστήματος
- Προσβάσεις στις ευαίσθητες πληροφορίες και τα συστήματα
- Τροποποιήσεις των δικαιωμάτων και των ελέγχων πρόσβασης
- Πρόσθετα συμβάντα σχετικά με την ασφάλεια

2) Κατ' ελάχιστο, οι ακόλουθες συναλλαγές πρέπει να καταγραφούν για κάθε εφαρμογή:

- Τροποποιήσεις στην εφαρμογή
- Ειδοποιήσεις και μηνύματα λάθους εφαρμογής
- Είσοδος και έξοδος των χρηστών
- Δραστηριότητες διαχείρισης συστήματος
- Προσβάσεις στις ευαίσθητες πληροφορίες
- Τροποποιήσεις των δικαιωμάτων και των ελέγχων πρόσβασης

3) Κατ' ελάχιστο, οι ακόλουθες συναλλαγές πρέπει να καταγραφούν για κάθε δρομολογητή, firewall ή άλλη σημαντική συσκευή δικτύων:

- Εκκίνηση και κλείσιμο της συσκευής
- Σύνδεση και έξοδος του διαχειριστή από το σύστημα
- Αλλαγές διαμόρφωσης
- Δημιουργία, τροποποίηση ή διαγραφή λογαριασμού
- Τροποποιήσεις των δικαιωμάτων και των ελέγχων πρόσβασης
- Ειδοποιήσεις και μηνύματα λάθους

4) Ο τύπος του συμβάντος, η ημερομηνία, η ώρα και το αναγνωριστικό χρηστών πρέπει να σημειώνονται για κάθε καταγεγραμμένη συναλλαγή.

5) Οι ευαίσθητες πληροφορίες, όπως οι κωδικοί πρόσβασης και τα δεδομένα Συστημάτων, δεν πρέπει να αποθηκεύονται στα αρχεία καταγραφής.

b) Η περιοδική επισκόπηση των εγγραφών ελέγχου θα διενεργούνται από το Τμήμα Ασφάλειας ή άλλο οριζόμενο προσωπικό.

c) Μόνο το οριζόμενο προσωπικό πρέπει να έχει πρόσβαση στις εγγραφές ελέγχου.

d) Τα αρχεία εγγραφών ελέγχου θα διατηρούνται για τουλάχιστον δύο (2) μήνες.

1) Οι εγγραφές ελέγχου που σχετίζονται με γνωστά συμβάντα (συμπεριλαμβανομένων εκείνων των εγγραφών που χρησιμοποιούνται για νομική δράση) θα διατηρούνται για δύο (2) μήνες.

e) Τα αρχεία των εγγραφών ελέγχου πρέπει να φυλάσσονται σε ασφαλή τοποθεσία. Τα δεδομένα εγγραφών ελέγχου πρέπει να είναι από τα πιο προσεκτικά φυλασσόμενα δεδομένα τοπικά αλλά και στα εφεδρικά αντίγραφα.

4.2 Ρόλοι & Υπευθυνότητες

- Οι ιδιοκτήτες πληροφοριών φέρουν την ευθύνη για τη διασφάλιση ότι οι εγγραφές ελέγχου εφαρμόζονται και διατηρούνται για τους πόρους τους.

- Οι διαχειριστές συστημάτων φέρουν την ευθύνη για την παροχή βοήθειας στους ιδιοκτήτες των πληροφοριών με την εφαρμογή και τη διατήρηση των εγγραφών ελέγχου για τους πόρους που είναι υπεύθυνοι.
- Οι προϊστάμενοι φέρουν την ευθύνη για την παροχή βοήθειας στο Τμήμα Ασφάλειας με τη διευθέτηση των ανωμαλιών στις εγγραφές ελέγχου.
- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την περιοδική επισκόπηση των εγγραφών ελέγχου όλων των συστημάτων για να διασφαλιστεί η συμμόρφωση με την παρούσα πολιτική.
- Οι χρήστες πληροφοριών πρέπει να κατανοήσουν και να αναγνωρίσουν ότι η χρήση συστημάτων της Εταιρείας μπορεί να καταγραφεί και να ελεγχθεί.

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

III. ΠΟΛΙΤΙΚΗ ΑΠΟΔΕΚΤΗΣ ΧΡΗΣΗΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

1.0 Εισαγωγή

Η Πολιτική Αποδεκτής Χρήσης ρυθμίζει τα θέματα που αφορούν στη χρήση των Πληροφοριακών Συστημάτων που υποστηρίζει τις δραστηριότητες της Εταιρείας. Η πολιτική αυτή συμβάλει στο να γνωρίζουν οι χρήστες ποιες ενέργειές τους θεωρούνται επιτρεπτές και ποιες μη επιτρεπτές.

Η αποτελεσματική ασφάλεια είναι μια συλλογική προσπάθεια που στηρίζεται στη συμμετοχή και την υποστήριξη του κάθε μέλους του προσωπικού που χειρίζεται πληροφορίες ή/και πληροφοριακά συστήματα.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι:

- Η αποτροπή πιθανών επιβλαβών συμβάντων που μπορεί να προκύψουν από κακή χρήση του ΟΠΣ της Εταιρείας.
- Η προστασία των χρηστών από τις συνέπειες που μπορεί να υποστούν από την εσφαλμένη χρήση του ΟΠΣ.
- Η διασφάλιση ότι οι χρήστες δεν θα καταχραστούν τις δυνατότητες χρήσης που τους παρέχονται προκειμένου να προβούν σε παράνομες ενέργειες.

3.0 Πεδίο Εφαρμογής

Η πολιτική αυτή απευθύνεται στα μέλη του προσωπικού της Εταιρείας και στους συνεργάτες της Εταιρείας που χρησιμοποιούν και υποστηρίζουν δραστηριότητες της Allweb Solutions S.A.

Η Διεύθυνση Ανθρώπινου Δυναμικού στις ενέργειες πρόσληψης προσωπικού ή συνεργατών τούς κοινοποιεί την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας και εξασφαλίζει με τη "Δήλωση Εργαζομένου" ότι έχουν λάβει γνώσει και αποδεχτεί την Πολιτική αυτή.
Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας.

4.0 Πολιτική

4.1 Γενική Χρήση και Ιδιοκτησία

1. Τα Πληροφοριακά Συστήματα συγκαταλέγονται στους πολυτιμότερους πόρους της Εταιρείας και κάθε μέλος του προσωπικού έχει την υποχρέωση να τα χρησιμοποιεί με σύνεση.
2. Τα Πληροφοριακά Συστήματα που προσφέρονται στο προσωπικό της Εταιρείας αποτελούν περιουσιακό της στοιχείο και η χρήση τους πρέπει να γίνεται αποκλειστικά για τους σκοπούς της Εταιρείας.
3. Η χρήση των Πληροφοριακών Συστημάτων συνεπάγεται την ανάληψη ευθυνών και υποχρεώσεων που περιγράφονται στην Πολιτική Αποδεκτής Χρήσης.

4.2 Δικαιώματα και Υποχρεώσεις Χρηστών

Οι παρακάτω δραστηριότητες παρέχουν ένα πλαίσιο με τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις του Πληροφοριακού Συστήματος.

4.2.1 Χρήση συστημάτων και δικτύων

1. Το προσωπικό πρέπει να χρησιμοποιεί το ΟΠΣ της Εταιρείας σύμφωνα με τα όσα προβλέπονται στην παρούσα Πολιτική Αποδεκτής Χρήσης.
2. Οι χρήστες οφείλουν να λαμβάνουν όλα τα μέτρα που υποδεικνύουν οι υπεύθυνοι της Εταιρείας για τη διασφάλιση του απορρήτου των επικοινωνιών τους.

   Η εταιρεία οφείλει να ενημερώνει τους χρήστες των παρεχόμενων υπηρεσιών τουλάχιστον κατά την σύναψη της μεταξύ τους σύβασης αλλά και σε τακτά χρονικά διαστήματα σχετικά με τα μέτρα που ενδείκνυται να λαμβάνουν για την προστασία του απορρήτου των επικοινωνιών τους, ιδίως σχετικά με κανόνες ορθής χρήσης των παρεχόμενων υπηρεσιών αλλά και τους τρόπους χρήσης τεχνολογιών και πόρων σχετικών με την ασφάλεια των πληροφοριών που σχετίζονται με τη διασφάλιση του απορρήτου των επικοινωνιών.
4. Τα εφεδρικά αντίγραφα πρέπει να τυγχάνουν μεταχείρισης του ιδίου επιπέδου κρισιμότητας και ευαισθησίας με τα δεδομένα και τις εφαρμογές που αποθηκεύονται σ' αυτά.
5. Τα εφεδρικά αντίγραφα πρέπει να μεταφέρονται σε μια ασφαλή, περιβαλλοντικά-ελεγχόμενη τοποθεσία εκτός του κτηρίου που φιλοξενεί το Μηχανογραφικό Κέντρο της Εταιρείας.
6. Κάθε σύστημα πρέπει να έχει ένα καθορισμένο πρόγραμμα διατήρησης εφεδρικών αντιγράφων που θα συμμορφώνεται με τις πολιτικές διατήρησης δεδομένων της Εταιρείας.
7. Περιοδικά πρέπει να εξετάζονται οι διαδικασίες λήψης εφεδρικών αντιγράφων και ανάκτησης δεδομένων από εφεδρικά αντίγραφα για να διασφαλιστεί ότι τα δεδομένα μπορούν να ανακτηθούν αποτελεσματικά από τα εφεδρικά αντίγραφα.
8. Η εταιρεία οφείλει να καταγράψει και να εφαρμόσει λεπτομερείς διαδικασίες για τη διεξαγωγή της λήψης εφεδρικών αντιγράφων, την ανάκτηση δεδομένων, την διεξαγωγή εξέτασης των εφεδρικών αντιγράφων, τη μεταφορά των ταινιών από/προς τις εγκαταστάσεις αποθήκευσης και την ανακύκλωση ή εξουδετέρωση των εφεδρικών αντιγράφων με τη πάροδο της περιόδου διατήρησής τους. Σκοπός των ενεργειών αυτών είναι η αποτροπή αποκάλυψης δεδομένων επικοινωνίας των χρηστών των παρεχόμενων υπηρεσιών σε μη εξουσιοδοτημένα άτομα.
9. Οι χρήστες οφείλουν να ενημερώνουν άμεσα το Τμήμα Ασφάλειας αν υποπέσει στην αντίληψή τους οποιοδήποτε κενό ασφάλειας συστήματος που θέτει σε κίνδυνο το απόρρητο επικοινωνιών των ίδιων ή άλλων χρηστών.
10. Οι χρήστες υποχρεούνται να συμμορφώνονται με την νομοθεσία για την προστασία της πνευματικής ιδιοκτησίας.
11. Οι χρήστες δεν επιτρέπεται να συμμετέχουν σε οποιαδήποτε παράνομή δραστηριότητα, βάσει εθνικού ή ευρωπαϊκού δικαίου, κάνοντας χρήση των πληροφοριακών πόρων της Εταιρείας.
12. Δεν επιτρέπεται η χρήση λογισμικού που δεν έχει αποκτηθεί με νόμιμο τρόπο.
13. Δεν επιτρέπεται η χρήση οποιουδήποτε υλικού ή λογισμικού που δεν είναι σε γνώση της Δοίκησης.
14. Η εγκατάσταση υλικού και λογισμικού στους Η/Υ των χρηστών γίνεται από τους ίδιους τους χρήστες με βάση τις παρούσες αρχές.
15. Οι χρήστες μεταβάλλου τους ελέγχους πρόσβασης (access controls), όταν αυτοί είναι ανεπαρκείς για την αποδοτική εργασία τους.

16. Δεν επιτρέπεται οποιαδήποτε ενέργεια μη εξουσιοδοτημένης χαρτογράφησης του δικτύου και η διεξαγωγή οποιασδήποτε μορφής παρακολούθησης του δικτύου της Εταιρείας.
17. Δεν επιτρέπεται η χρήση υπολογιστικών συστημάτων που δεν ανήκουν στην Εταιρεία για εργασίες της Εταιρείας.
18. Τα μέλη του προσωπικού που διαθέτουν φορητό υπολογιστή, ο οποίος παρέχεται από την Εταιρεία και χρησιμοποιείται για εργασιακούς σκοπούς, πρέπει να συμμορφώνονται με τις πολιτικές που ισχύουν για το σχετικό εξοπλισμό (Πολιτική Φορητών Υπολογιστών).
19. Δεν επιτρέπεται η εισαγωγή κακόβουλων προγραμμάτων στο δίκτυο ή τους κεντρικούς υπολογιστές (π.χ., ιοί, σκουλήκια, Δούρειοι Ίπποι, e-mail bombs, κ.λπ.).
20. Όλοι οι υπολογιστές που χρησιμοποιούνται από υπαλλήλους που συνδέονται με το Internet/Intranet/Extranet της Εταιρείας πρέπει να εκτελούν συνεχώς το εγκεκριμένο λογισμικό ανίχνευσης ιών με μια ενημερωμένη βάση δεδομένων ιών.
21. Όλοι οι υπολογιστές πρέπει να κάνουν χρήση της λειτουργία προφύλαξης οθόνης (screensaver) με προστασία κωδικού πρόσβασης ή να γίνεται κλείδωμά του ηλεκτρονικού υπολογιστή κατά την απομάκρυνση του χρήστη.
22. Οι χρήστες υποχρεούνται να συμμορφώνονται με την εκάστοτε ισχύουσα "Πολιτική Κωδικών Πρόσβασης" για τη σωστή επιλογή και διαχείριση αυτών.

4.2.2 Χρήση Ηλεκτρονικού Ταχυδρομείου και Παγκοσμίου Ιστού

1. Η πρόσβαση στο Διαδίκτυο παρέχεται στο προσωπικό της Εταιρείας για να χρησιμοποιηθεί για τους σκοπούς της Εταιρείας και για τη βελτίωση των γνώσεων και δεξιοτήτων του ανθρώπινου δυναμικού της.
2. Η Εταιρεία διατηρεί το δικαίωμα να περιορίσει την πρόσβαση σε συγκεκριμένους Ισοτόπους (Web Sites) του Παγκόσμιου Ιστού (World Wide Web). Οι χρήστες που χρειάζονται πρόσβαση σε Ισοτόπους που η πρόσβαση έχει περιοριστεί έχουν το δικαίωμα να υποβάλλουν σχετικό αίτημα.
3. Οι χρήστες πρέπει να γνωρίζουν ότι οι δυνατότητες των γραμμών που συνδέουν την Εταιρεία με το Διαδίκτυο είναι πεπερασμένες και κατά συνέπεια η κατάχρηση των υπηρεσιών του Διαδικτύου (πχ. η λήψη μεγάλων αρχείων) περιορίζει τη χρήση του Διαδικτύου από τους συναδέλφους τους.
4. Οι χρήστες πρέπει να αποφεύγουν την επίσκεψη σε Ιστοσελίδες (Web Pages) με παράνομο λογισμικό ή άλλο πειρατικό οπτικοακουστικό υλικό. Οι χρήστες πρέπει να γνωρίζουν ότι η επίσκεψη αυτών των Ιστοσελίδων μπορεί να θέσει σε κίνδυνο την ασφάλεια του Πληροφοριακού Συστήματος.

5.0 Παρακολούθηση και έλεγχος εφαρμογής της πολιτικής

1. Τα δεδομένα που δημιουργούνται με τη χρήση του Πληροφοριακού Συστήματος της Εταιρείας αποτελούν ιδιοκτησία της Εταιρείας.
2. Για την διασφάλιση της καλής και ασφαλούς λειτουργίας των πόρων του Πληροφοριακού Συστήματος, η χρήση τους μπορεί να καταγράφεται από εξουσιοδοτημένα άτομα (π.χ. διαχειριστές συστημάτων και δικτύων). Η καταγραφή δεν αφορά το περιεχόμενο της ηλεκτρονικής μετάδοσης πληροφοριών.
3. Η Εταιρεία διατηρεί το δικαίωμα να διενεργεί προγραμματισμένους ή έκτακτους ελέγχους για την τήρηση της Πολιτικής Αποδεκτής Χρήσης και για την τήρηση των πολιτικών που συμπεριλαμβάνονται στην ευρύτερη Πολιτική Ασφάλειας της Εταιρείας. Τους ελέγχους πραγματοποιούν εξουσιοδοτημένα για το σκοπό αυτό άτομα (Ελεγκτές Πληροφοριακών Συστημάτων) και τα μέλη του προσωπικού οφείλουν να συνεργαστούν μαζί τους. Το προσωπικό έχει δικαίωμα να ενημερωθεί για τα μέσα ελέγχου, τα κριτήρια ελέγχου και τα αποτελέσματα των ελέγχων που το αφορούν.

6.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας αποτελεί ευθύνη του Τμήματος Ασφάλειας.

7.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

IV. ΠΟΛΙΤΙΚΗ ΕΚΠΑΙΔΕΥΣΗΣ ΚΑΙ ΕΝΗΜΕΡΩΣΗΣ (Security Training and Awareness)

1.0 Εισαγωγή

Η εκπαίδευση και ενημέρωση του προσωπικού σε θέματα ασφάλειας είναι αποφασιστικής σημασίας για την προστασία των πληροφοριακών πόρων της Εταιρείας. Οι πολιτικές ασφάλειας και τα πρότυπα μπορούν να είναι αποτελεσματικά μόνο αν κάθε μέλος του προσωπικού της Εταιρείας, ανεξάρτητα από τη θέση στην Εταιρεία, αναγνωρίζει τη σημασία της ασφάλειας, καταλαβαίνει τις διαδικασίες ασφάλειας της Εταιρείας και ακολουθεί τις απαραίτητες πρακτικές.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι να διασφαλιστεί ότι οι χρήστες, που εμπλέκονται κατά τη διάρκεια της εργασίας τους με τα Πληροφοριακά και Επικοινωνιακά Συστήματα, έχουν τις απαιτούμενες γνώσεις και τα εφόδια για να εφαρμόσουν και να υποστηρίξουν την Πολιτική Ασφάλειας.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλο το προσωπικό (μόνιμο ή προσωρινό) της Εταιρείας και τους αναδόχους που έχουν πρόσβαση στους πληροφοριακούς πόρους της Εταιρείας.

4.0 Πολιτική

4.1 Διαδικασίες & Οδηγίες

a) Η Διοίκηση μεριμνά για την εκπαίδευση και ευαισθητοποίηση σε θέματα ασφάλειας των χρηστών και γενικά του προσωπικού της Εταιρείας που σχετίζεται με τη λειτουργία των ΟΠΣ.

b) Η Διοίκηση μεριμνά για την κατάρτιση σε θέματα ασφάλειας ΟΠΣ των διαχειριστών των συστημάτων και ειδικότερα των στελεχών που αναλαμβάνουν ρόλους σχετικούς με την ασφάλεια.

c) Η Διοίκηση μεριμνά ώστε να είναι διαθέσιμες στο προσωπικό πηγές πληροφόρησης για ζητήματα ασφάλειας, καθώς και εκπαιδευτικό υλικό, όπως μαθήματα από απόσταση, εκπαιδευτικά video κλπ.

d) Η εταιρεία οφείλει να παρέχει στο προσωπικό της (μόνιμο ή προσωρινό), στους προμηθευτές υπηρεσιών καθώς και στους αναδόχους έργων που μπορεί να επηρεάσουν την ασφάλεια των ΟΠΣ πλήρη πρόσβαση στην Πολιτική Ασφάλειας για την Διασφάλιση των Επικοινωνιών της εταιρείας.

e) Όλα τα νέα μέλη του προσωπικού πρέπει να ακολουθούν ένα βασικό πρόγραμμα εκπαίδευσης και ενημέρωσης, το οποίο Περιλαμβάνει και ζητήματα ασφάλειας ΟΠΣ.

f) Τα διοικητικά στελέχη της Εταιρείας αποδεικνύουν την αυξημένη σημασία που έχει η ασφάλεια των ΟΠΣ, εφαρμόζοντας υποδειγματικά την Πολιτική Ασφάλειας και τις διαδικασίες ασφάλειας που απορρέουν από αυτήν.

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

V. ΠΟΛΙΤΙΚΗ ΑΝΑΔΟΧΩΝ ΚΑΙ ΣΥΝΕΡΓΑΤΩΝ

1.0 Εισαγωγή

Οι δραστηριότητες των συνεργατών της Allweb Solutions S.A, είτε πρόκειται για φυσικά πρόσωπα είτε για εταιρείες που αναλαμβάνουν διάφορες εργασίες, όπως εργασίες ανάπτυξης και συντήρησης συστημάτων, εκτυπωτικές εργασίες κλπ., καθώς και των προμηθευτών υπηρεσιών, όπως οι τηλεπικοινωνιακές υπηρεσίες, μπορεί να θέσουν σε κίνδυνο την εφαρμογή της Πολιτικής Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων της Εταιρείας.
Η Εταιρεία διατηρεί την ευθύνη απέναντι στο Νόμο για την παραβίαση του απορρήτου των επικοινωνιών ή την κατάχρηση των προσωπικών δεδομένων των πελατών όταν αυτή προέλθει από συνεργάτες της Εταιρείας ή από αναδόχους εργασιών. Για τους ανωτέρω λόγους πρέπει να διασφαλίζεται ότι οι ανάδοχοι και οι συνεργάτες συμμορφώνονται και εφαρμόζουν τα όσα ορίζει η Πολιτική Ασφάλειας.

2.0 Σκοπός

Σκοπός της Πολιτικής Αναδόχων και Συνεργατών είναι:

- Η αποτροπή πιθανών επιβλαβών συμβάντων που μπορεί να προκύψουν από τις δραστηριότητες των αναδόχων και των συνεργατών της Εταιρείας.
- Να διασφαλιστεί ότι προστατεύονται τα προσωπικά δεδομένα και το απόρρητο των επικοινωνιών των πελατών της Allweb Solutions S.A.

3.0 Πεδίο εφαρμογής

Η πολιτική αφορά τους συνεργάτες της Allweb Solutions S.A., είτε πρόκειται για φυσικά, είτε για νομικά πρόσωπα που έχουν ή μπορεί να έχουν πρόσβαση στα ΟΠΣ ή στις πληροφορίες που συλλέγει και επεξεργάζεται η Allweb Solutions S.A. Επίσης, αφορά αναδόχους εργασιών και προμηθευτές υπηρεσιών που έχουν ή μπορεί να έχουν πρόσβαση στα ΟΠΣ ή στις πληροφορίες που συλλέγει και επεξεργάζεται η Allweb Solutions S.A.. Οι συνεργάτες / προμηθευτές μπορεούν να παρέχουν υπηρεσίες και μέσω cloud IAAS (Infrasrructure As A Service), PAAS (Platform As A Service), SAAS (Software As A Service). Η εφαρμογή της πολιτικής είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της σύβασης συνεργασίας.

4.0 Πολιτική

4.1 Γενικές Αρχές

- **Υποχρεώσεις αναδόχων και συνεργατών**
  Οι συνεργάτες της εταιρείας και οι ανάδοχοι εργασιών έχουν τις ίδιες υποχρεώσεις αναφορικά με την ασφάλεια που έχει και το προσωπικό της Εταιρείας.

- **Διασφάλιση απορρήτου των επικοινωνιών**
  - Η Εταιρεία προβαίνει σε όλες τις ενέργειες που διασφαλίζουν ότι οι δραστηριότητες των αναδόχων και των συνεργατών δεν θέτουν σε κίνδυνο τα δικαιώματα των πελατών της

αναφορικά με την προστασία των προσωπικών τους δεδομένων και τη διασφάλιση του απορρήτου των επικοινωνιών.

- Η Εταιρεία οφείλει να διατηρεί ενημερωμένο αρχείο στο οποίο καταγράφονται οι συνεργάτες, οι οποίοι προκειμένου να παράσχουν τις υπηρεσίες τους, αποκτούν ή δύναται να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών.

- **Προστασία ΟΠΣ από ενέργειες αναδόχων και συνεργατών**
  Η Εταιρεία αναγνωρίζει τους κινδύνους που προέρχονται από τις δραστηριότητες των συνεργατών της και των αναδόχων εργασιών και λαμβάνει όλα τα μέτρα ώστε να τους περιορίσει.

4.2 Οδηγίες & κανόνες ασφάλειας

4.2.1 Υποχρεώσεις Αναδόχων και Συνεργατών

- Οι ανάδοχοι εργασιών και οι συνεργάτες της Εταιρείας οφείλουν να γνωρίζουν και να εφαρμόζουν την Πολιτική Ασφάλειας της Εταιρείας. Για το προσωπικό των αναδόχων που εκτελούν εργασίες στις εγκαταστάσεις της Εταιρείας ισχύουν οι ίδιοι κανόνες με το προσωπικό της Εταιρείας.
- Οι ανάδοχοι εργασιών και οι συνεργάτες της Εταιρείας οφείλουν να αναφέρουν κάθε περιστατικό που μπορεί να θέσει σε κίνδυνο τα ΟΠΣ της Εταιρείας.
- Οι ανάδοχοι εργασιών και οι συνεργάτες της Εταιρείας οφείλουν να διατηρούν την εμπιστευτικότητα των δεδομένων στα οποία αποκτούν πρόσβαση.
- Οι ανάδοχοι εργασιών και οι συνεργάτες της Εταιρείας απαγορεύεται να αποκαλύπτουν πληροφορίες ή άλλα στοιχεία που συνδέονται με (α) το περιεχόμενο ή την ουσία των επικοινωνιών των πελατών της, (β) στοιχεία σχετικά με υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα πρόσωπο ή (γ) άλλα προσωπικά δεδομένα χρηστών των τηλεπικοινωνιακών υπηρεσιών, όπως αριθμούς τηλεφώνου ή διευθύνσεις.

4.2.2 Προκηρύξεις Διαγωνισμών και Συμβάσεις

- Οι συμβάσεις έργων που σχετίζονται με τη λειτουργία των ΟΠΣ της Εταιρείας περιλαμβάνουν όρους που εξασφαλίζουν συμβατικά και τεχνικά την τήρηση της Πολιτικής Ασφάλειας της Εταιρείας. Στις συβάσεις γίνεται ιδιαίτερη αναφορά στην τήρηση της Πολιτικής Απορρήτου και Προστασίας Προσωπικών Δεδομένων της Εταιρείας
- Οι συβάσεις έργων που σχετίζονται με τη λειτουργία των ΟΠΣ της Εταιρείας περιλαμβάνουν ρήτρες σε περίπτωση μη συμμόρφωσης με την Πολιτική Ασφάλειας της Εταιρείας.
- Για την πρόσβαση σε προσωπικά δεδομένα πελατών ή σε δεδομένα που αφορούν τις επικοινωνίες των πελατών της
- Allweb Solutions S.A. απαιτείται η λήψη άδειας από τον Υπεύθυνο Ασφάλειας.
- Ο Υπεύθυνος Ασφάλειας οφείλει να ελέγχει και να γνωμοδοτεί για την επάρκεια των όρων της σύβασης σε σχέση με την ασφάλεια, όπως επίσης και για τη δυνατότητα του αναδόχου ή συνεργάτη να ανταποκριθεί στις απαιτήσεις ασφάλειας που θέτει η Εταιρεία.
- Η Εταιρεία ορίζει συγκεκριμένο φυσικό πρόσωπο που είναι υπεύθυνο για τη εποπτεία του εκάστοτε συνεργάτη ή/και αναδόχου.
- Οι όροι που αφορούν την τήρηση της Πολιτικής Ασφάλειας περιλαμβάνονται και στις προκηρύξεις των έργων.
- Για το προσωπικό των αναδόχων και συνεργατών που έχουν πρόσβαση στις εγκαταστάσεις και το δικτυακό εξοπλισμό της Εταιρείας απαιτείται ενυπόγραφη άδεια από τον Υπεύθυνο Ασφάλειας της Εταιρείας.
- Τα άτομα που πραγματοποιούν εργασίες στα ΟΠΣ. της Εταιρείας καταγράφονται και η ταυτότητά τους ελέγχεται.
- Εξωτερικά συνεργεία συντήρησης, επισκευών και καθαρισμού συνοδεύονται διαρκώς από άτομα της Εταιρείας όταν βρίσκονται σε ευαίσθητους χώρους.
- Ο ανάδοχος έργου δεν μπορεί να εκχωρήσει δικαιώματα χρήσης του ευαίσθητου εξοπλισμού σε τρίτους χωρίς ενυπόγραφη άδεια της Εταιρείας.

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

VI. ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΕΦΕΔΡΙΚΩΝ ΑΝΤΙΓΡΑΦΩΝ

1.0 Εισαγωγή

Υπάρχουν πολλές απειλές που θα μπορούσαν να προκαλέσουν απώλεια, φθορά ή προσωρινή μη-διαθεσιμότητα των δεδομένων. Αυτές περιλαμβάνουν, ενδεικτικά και όχι περιοριστικά, αστοχίες υλικού, τυχαία διαγραφή, λανθασμένη τροποποίηση, φθορά λογισμικού και κακόβουλες ενέργειες. Οι προαναφερόμενες απειλές είναι πολύ κοινές και αναπόφευκτα μερικές από αυτές θα εμφανιστούν περιστασιακά στην Εταιρεία.

Είναι επομένως αναγκαίο η Εταιρεία να διατηρεί εφεδρικά αντίγραφα όλων των κρίσιμων δεδομένων και συστημάτων έτσι ώστε να μπορούν να χρησιμοποιηθούν για να παρέχουν συνεχή διαθεσιμότητα και βιωσιμότητα αυτών των πόρων όταν εμφανίζονται τέτοια περιστατικά.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι τα εφεδρικά αντίγραφα των κρίσιμων πληροφοριακών πόρων της Εταιρείας να διεκπεραιώνονται, να ελέγχονται και να διαχειρίζονται κατάλληλα.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλους τους πληροφοριακούς πόρους της Εταιρείας.

4.0 Πολιτική

4.1 Διαδικασίες & οδηγίες

- Πρέπει να γίνεται λήψη εφεδρικών αντιγράφων όλων των κρίσιμων πληροφοριακών πόρων της Εταιρείας.
- Τα εφεδρικά αντίγραφα πρέπει να αποθηκεύονται μόνο σε αναγνώσιμά αρχεία.
- Η λήψη εφεδρικών αντιγράφων πρέπει να εκτελείται σύμφωνα με το ακόλουθο πρόγραμμα:
    - Λήψη εφεδρικών αντιγράφων για όλα τα κρίσιμα δεδομένα και τη διάρθρωση των Συστημάτων τουλάχιστον σε καθημερινή βάση.
    - Λ ή ψ η εφεδρικών αντιγράφων των εφαρμογών και των αδειών όποτε υπάρχουν αλλαγές σ' αυτές.
    - Η λήψη εφεδρικών αντιγράφων των μη-κρίσιμων δεδομένων επαφίεται στην κρίση του κατόχου των δεδομένων.
- Τα εφεδρικά αντίγραφα πρέπει να μεταφέρονται σε μια ασφαλή, περιβαλλοντικά-ελεγχόμενη τοποθεσία εκτός του κτηρίου γραφείων της Εταιρείας.

- Κάθε σύστημα πρέπει να έχει ένα καθορισμένο πρόγραμμα διατήρησης εφεδρικών αντιγράφων που θα συμμορφώνεται με τις πολιτικές διατήρησης δεδομένων της Εταιρείας.
- Περιοδικά πρέπει να εξετάζονται οι διαδικασίες λήψης εφεδρικών αντιγράφων και ανάκτησης δεδομένων από εφεδρικά αντίγραφα για να διασφαλιστεί ότι τα δεδομένα μπορούν να ανακτηθούν αποτελεσματικά από τα εφεδρικά αντίγραφα.
- Πρέπει να σχεδιαστούν και να εφαρμοστούν λεπτομερείς διαδικασίες για τη διεξαγωγή της λήψης εφεδρικών αντιγράφων, την ανάκτηση δεδομένων, την διεξαγωγή εξέτασης των εφεδρικών αντιγράφων, τη μεταφορά των ταινιών από/προς τις εγκαταστάσεις αποθήκευσης και την ανακύκλωση ή εξουδετέρωση των εφεδρικών αντιγράφων με τη πάροδο της περιόδου διατήρησής τους.
- Τα εφεδρικά αντίγραφα πρέπει να τυγχάνουν μεταχείρισης του ιδίου επιπέδου κρισιμότητας και ευαισθησίας με τα δεδομένα και τις εφαρμογές που αποθηκεύονται σ' αυτά.
- Οι διαχειριστές Συστημάτων πρέπει να κάνουν λήψη εφεδρικών αντιγράφων των δεδομένων που αποθηκεύονται στους κεντρικούς υπολογιστές. Ωστόσο, οι χρήστες είναι υπεύθυνοι για τη λήψη εφεδρικών αντιγράφων των δεδομένων που αποθηκεύονται στους σταθμούς εργασίας τους και τα φορητά μέσα αποθήκευσης (δηλ., δισκέτες, CDs,DVDs κλπ...).
    - Οι χρήστες μπορούν να αντιγράψουν τα δεδομένα τους στους κεντρικούς υπολογιστές, στους οποίους γίνεται λήψη εφεδρικών αντιγράφων, ή μπορούν να κάνουν οι ίδιοι λήψη εφεδρικών αντιγράφων των δεδομένων τους που δεν αποθηκεύονται στους κεντρικούς υπολογιστές της Εταιρείας.

4.2 Ρόλοι & Υπευθυνότητες

- Οι ιδιοκτήτες πληροφοριών πρέπει να διασφαλίσουν ότι γίνεται λήψη εφεδρικών αντιγράφων των πόρων τους σύμφωνα με την παρούσα πολιτική.
- Οι διαχειριστές Συστημάτων πρέπει να βοηθήσουν τους ιδιοκτήτες πληροφοριών με τη λήψη και διαχείριση εφεδρικών αντιγράφων και την ανάκτηση των δεδομένων τους απ' αυτά.
- Το Τμήμα Ασφάλειας πρέπει να διεξάγει ελέγχους για να διασφαλίσει τη συμμόρφωση με την παρούσα πολιτική.
- Οι χρήστες πρέπει να εξασφαλίσουν ότι για οποιαδήποτε κρίσιμα δεδομένα που αποθηκεύονται στους σταθμούς εργασίας τους ή τα φορητά μμέσα τους γίνεται λήψη εφεδρικών αντιγράφων σύμφωνα με την παρούσα πολιτική.

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	Ημερομηνία	Αλλαγές
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

VII. ΠΟΛΙΤΙΚΗ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ (Physical and Environmental Security)

1.0 Εισαγωγή

Δεν είναι ιδιαίτερα κρίσιμο για την Εταιρεία να εφαρμόζει μέτρα προστασίας φυσικής ασφάλειας για την προστασία των πληροφοριακών της πόρων κάθως οι κρίσιμες πληροφορίες βρίσκονται σε cloud υπηρεσίες. Παρόλα αυτά λαμβάνονται μέτρα και εφαρμόζονται σε όλους τους χώρους και μπορεί να περιλαμβάνουν τη χρήση κλειδαριών, διοικητικών ελέγχων και μέτρων για την προστασία από τη ζημία που προέρχεται από σκόπιμές πράξεις, ατυχήματα, πυρκαγιές και περιβαλλοντικούς κινδύνους.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι να οριστούν τα φυσικά μέτρα ασφάλειας για τους πληροφοριακούς πόρους ώστε να διασφαλιστεί η κατάλληλη και έγκαιρη λειτουργία τους, να προστατευθεί η αξία τους, να προστατευθεί η ακεραιότητα των πληροφοριών και να διασφαλιστεί η ασφάλεια του προσωπικού. Τα συστήματα ηλεκτρονικών υπολογιστών, οι εγκαταστάσεις και οι περιοχές αποθήκευσης εφεδρικών αντιγράφων πρέπει να προστατεύονται από τον κίνδυνο κλοπής και μεταβολής, τις ζημιές από πυρκαγιά, τη σκόνη, το νερό, την διακοπή ηλεκτρικού ρεύματος καθώς και τη μη εξουσιοδοτημένη διάσπαση της λειτουργίας.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ορίζει τις διαδικασίες, τις οδηγίες και τα πρότυπα που αφορούν την εφαρμογή των φυσικών μέτρων ασφάλειας με σκοπό να προστατεύσουν τους πληροφοριακούς πόρους της Εταιρείας. Δεν αφορά την προστασία του προσωπικού, των εγκαταστάσεων και της περιουσίας που δεν συνδέεται άμεσα με τις τεχνολογίες πληροφορικής.

4.0 Πολιτική

4.1 Διαδικασίες & Οδηγίες

α) Η φυσική πρόσβαση στους πληροφοριακούς πόρους πρέπει να ελέγχεται ανάλογα της κατηγοριοποίησης του πόρου και το επίπεδο κινδύνου.

β) Οι χώροι που φιλοξενούν ευαίσθητους πληροφοριακούς πόρους απαιτούν ειδικά μέτρα προστασίας για να περιοριστεί η πρόσβαση σε αυτούς τους πόρους.

γ) Οι χώροι που φιλοξενούν κρίσιμους πληροφοριακούς πόρους πρέπει να τυγχάνουν ειδικών μέτρων προστασίας ώστε να διασφαλιστεί η διαθεσιμότητα αυτών των πόρων, πρέπει να εφαρμόζονται μέτρα προστασίας ενάντια στις πυρκαγιές, τις πλημμύρες, την υγρασία και άλλους περιβαλλοντικούς παράγοντες που θα μπορούσαν να βλάψουν τους πόρους.

δ) Τα εφεδρικά αντίγραφα και άλλα μέσα, πρωτότυπα και αντίγραφα, που περιέχουν δεδομένα και προγράμματα πρέπει να διατηρούνται σε καλή κατάσταση και να προστατεύονται από κλοπή. Είναι σημαντικό τα εφεδρικά αντίγραφα ασφάλειας να φυλάσσονται σε μια διαφορετική τοποθεσία από τα πρωτότυπα.

4.2 Ρόλοι & Υπευθυνότητες

a) Οι χρήστες πληροφοριών φέρουν την ευθύνη για:

1) Την κατανόηση και τη συμμόρφωση με τις απαιτήσεις ασφάλειας που ορίζονται στην παρούσα πολιτική.

2) Την φυσική προστασία των πληροφοριακών πόρων της Εταιρείας που ανατίθενται στην κυριότητά τους.

3) Την αναφορά οποιουδήποτε περιστατικού ή κατάστασης που έρχεται σε αντίθεση με τις οριζόμενες απαιτήσεις στο Τμήμα Ασφάλειας.

b) Οι προϊστάμενοι φέρουν την ευθύνη για:

1) Τη διασφάλιση ότι το προσωπικό τους κατανοεί την πολιτική της Εταιρείας σχετικά με τη φυσική και περιβαλλοντική ασφάλεια.

2) Τη παρακολούθηση της συμμόρφωσης των υπαλλήλων τους με την παρούσα πολιτική.

c) Οι ιδιοκτήτες πληροφοριών φέρουν την ευθύνη για την εφαρμογή των μέτρων έτσι ώστε να προστατεύονται οι πόροι τους από τις φυσικές και περιβαλλοντικές απειλές καθώς και από μη εξουσιοδοτημένη φυσική πρόσβαση.

d) Οι υπεύθυνοι Συστημάτων φέρουν την ευθύνη για την παροχή βοήθειας στους ιδιοκτήτες πληροφοριών με την εφαρμογή των φυσικών και περιβαλλοντικών μέτρων ασφάλειας.

e) Το Τμήμα Ασφάλειας φέρει την ευθύνη της διεξαγωγής ελέγχων για να διασφαλιστεί η συμμόρφωση με την παρούσα πολιτική και οδηγίες.

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

VIII. ΠΟΛΙΤΙΚΗ ΛΟΓΙΚΗΣ ΠΡΟΣΒΑΣΗΣ

1.0 Εισαγωγή

Οι χρήστες πρέπει να έχουν πρόσβαση στους πληροφοριακούς πόρους που απαιτούνται για να διεκπεραιώσουν τις εργασίες τους. Εντούτοις, η υπερβολική ή η ανεξέλεγκτη πρόσβαση μπορεί να οδηγήσει στη μη εξουσιοδοτημένη ή ακούσια αποκάλυψη, τροποποίηση ή καταστροφή των πόρων, καθώς και στον καταλογισμό ευθύνης για αμέλεια στην προστασία των πόρων. Επομένως, η πρόσβαση σε συγκεκριμένους πόρους χορηγείται μόνο στο εξουσιοδοτημένο προσωπικό που έχει μια εύλογη ανάγκη να χρησιμοποιήσει αυτούς τους πόρους. Τα προνόμια πρόσβασης σ' αυτούς τους πόρους περιορίζονται σ' εκείνα που απαιτούνται για την εκτέλεση των καθηκόντων του εξουσιοδοτημένου προσωπικού.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι να περιοριστεί η πρόσβαση στους πληροφοριακούς πόρους της Εταιρείας μόνο στο προσωπικό που χρειάζεται τους συγκεκριμένους πόρους για να εκτελέσει τα καθήκοντά του. Οι αρχές του "διαχωρισμού των καθηκόντων" και "ελάχιστων δικαιωμάτων" πρέπει να εφαρμόζονται στην κατανομή των δικαιωμάτων πρόσβασης.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλους τους χρήστες, ιδιοκτήτες και διαχειριστές πληροφοριών καθώς και για οποιαδήποτε πρόσβαση στους πληροφοριακούς πόρους της Εταιρείας. Στην παρούσα πολιτική γίνεται ιδιαίτερη αναφορά για τον έλεγχο πρόσβασης που αφορά τους χρήστες της υπηρεσίας ηλεκτρονικού ταχυδρομείου και τις λοιπές υπηρεσίες που παρέχονται μέσω της διαδικτυακής πύλης της εταιρείας (http://www.allweb.gr)

4.0 Πολιτική

4.1 Διαδικασίες & Οδηγίες

- Στους χρήστες πρέπει να χορηγούνται συγκεκριμένα δικαιώματα πρόσβασης σε κάθε σύστημα, τα οποία πρέπει να περιορίζονται σε εκείνα που απαιτούνται για να εκτελέσουν τις εργασίες τους.
- Οι χρήστες πρέπει να έχουν την έγκριση του ιδιοκτήτη των πληροφοριών πριν από τη χορήγηση της πρόσβασης σε έναν επιμέρους πόρο.
- Οι χρήστες πρέπει να προσπελαύνουν μόνο τους πόρους για τους οποίους έχουν εξουσιοδότηση, ανεξάρτητα από τα πραγματικά δικαιώματα συστήματος.
- Οι χρήστες δεν πρέπει να παρακάμπτουν τα δικαιώματα που χορηγούνται στους λογαριασμούς τους προκειμένου να αποκτήσουν πρόσβαση σε μη εξουσιοδοτημένους πληροφοριακούς πόρους.
- Οι χρήστες πρέπει να προστατεύουν τους λογαριασμούς τους:
    - Δεν πρέπει να επιτρέπουν σε τρίτους να χρησιμοποιούν τον λογαριασμό τους ή να χρησιμοποιούν τους υπολογιστές τους όταν είναι συνδεδεμένοι με το λογαριασμό τους, εκτός εάν απαιτείται για τη διαχείριση του συστήματος.
    - Οι χρήστες φέρουν την ευθύνη για οποιαδήποτε δραστηριότητα λαμβάνει μέρος στο ΟΠΣ με τη χρήση του δικούς τους αναγνωριστικού ταυτότητας «user ID» (δεδομένου ότι μόνο αυτοί πρέπει να έχουν πρόσβαση στο userID τους).

- Όταν ο υπολογιστής τους είναι αφύλακτος, οι χρήστες είτε αποσυνδέονται είτε θέτουν σε λειτουργία την προστασία του συστήματος τους (όπως προφύλαξη οθόνης «screensaver» με κωδικό πρόσβασης).

- Το επίπεδο ελέγχου πρόσβασης εξαρτάται από την κατηγοριοποίηση του πόρου και το επίπεδο κινδύνου που συνδέεται με τον πόρο.
- Η εταιρεία οφείλει να καθιερώσει και να ακολουθεί διαδικασία διαχείρισης χρηστών στην οποία θα πρέπει να περιγράφονται τα παρακάτω:
  - ο τρόπος προσθήκης νέων χρηστών, η διαγραφή χρηστών καθώς και η αναμονή και μεταβολή δικαιωμάτων ή επιπέδων πρόσβασης
  - να προβλέπεται η υποχρέωση τήρησης αρχείου των αιτήσεων που αφορούν σε κάθε μεταβολή στην κατάσταση πρόσβασης των χρηστών
  - να προβλέπεται η υποχρέωση τήρησης αρχείου με το ιστορικό όλων των δικαιωμάτων ή επιπέδων πρόσβασης των λογαριασμών που έχουν εγκριθεί και ενεργοποιηθεί στα ΟΠΣ της εταιρείας
- Η εταιρεία οφείλει να καθιερώσει και να ακολουθεί διαδικασία ελέγχου ορθής εφαρμογής της Πολιτικής Λογικής Πρόσβασης όπου πρέπει να περιγράφονται οι περιοδικοί έλεγχοι που πραγματοποιούνται σε συμφωνία με τους υπεύθυνους για τον έλεγχο εφαρμογής της πολιτικής ασφάλειας της εταιρείας αναφορικά με :
  - Τον έλεγχο των δικαιωμάτων πρόσβασης των χρηστών, ήτοι, εάν το δικαίωμα πρόσβασης εκάστου χρήστη είναι πράγματι αυτό που του αποδοθεί.
  - Τον έλεγχο των λογαριασμών πρόσβασης, ήτοι, την αντιπαραβολή του αρχείου που περιλαμβάνει τις εγκεκριμένες αιτήσεις με τους λογαριασμούς που προκύπτουν.
  - Τον δειγματοληπτικό έλεγχο των αρχείων καταγραφής πρόσβασης για την ανακάλυψη ενδεχόμενων μη αιτιολογημένων προσβάσεων.
- Οι διαχειριστές Συστημάτων πρέπει να αναθεωρούν περιοδικά τα προνόμια χρηστών και να τα τροποποιούν, ανακαλούν ή απενεργοποιούν, ανάλογα με την περίπτωση, βάσει των ανωτέρω κριτηρίων.
- Η πρόσβαση στα Πληροφορικά Συστήματα της Εταιρείας ελέγχεται από κατάλληλους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης (π.χ όνομα χρήστη, κωδικός πρόσβασης, captha).
- Η εταιρεία οφείλει να διατηρεί αρχεία σε κάθε σχετική υπηρεσία με τις παρακάτω πληροφορίες:
  - οι προσβάσεις των χρηστών των ΟΠΣ
  - τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης για κάθε ΟΠΣ.
  - την αντιστοίχιση των λογαριασμών πρόσβασης των εργαζόμενων και συνεργατών στους οποίους αυτοί έχουν αποδοθεί, ούτως ώστε να είναι δυνατό να διαπιστώνεται ποιος είναι ο κάτοχος κάθε λογαριασμού πρόσβασης και για ποιο χρονικό διάστημα.
  - οι κατηγορίες των χρηστών και τα δικαιώματα πρόσβασης αυτών.
  - οι τρόποι πρόσβασης των εργαζομένων και συνεργατών σε δεδομένα επικοινωνίας των χρηστών των παρεχόμενων υπηρεσιών.
- Σχετικά με την δημιουργία και διαχείριση των λογαριασμών πρόσβασης , η εταιρεία οφείλει να διατηρεί τα ακόλουθα:
  - περιγραφή των κανόνων σύμφωνα με τους οποίους γίνεται η δημιουργία ενός ονόματος χρήστη.
  - Διαδικασία σύμφωνα με την οποία αποδίδεται με ασφάλεια σε κάθε εργαζόμενο και συνεργάτη της εταιρείας το όνομα χρήστη και ο κωδικός πρόσβασης που τον αφορά.
- Οι μηχανισμοί ελέγχου πρόσβασης καλύπτουν τα δεδομένα σε όλες τις μορφές τους, συμπεριλαμβανομένων των μαγνητικών ή οπτικών μέσων μεταφοράς, τα εφεδρικά αντίγραφα δεδομένών (back up), τα δεδομένα που μεταβιβάζονται μέσω δικτύων ή τηλεπικοινωνιακών γραμμών, δεδομένα σε έντυπη μορφή κλπ.

- Οι μηχανισμοί ελέγχου πρόσβασης διασφαλίζουν ότι υπάρχει δυνατότητα ταυτοποίησης του ατόμου που πραγματοποίησε μία ενέργεια. Η αρχή αυτή ισχύει τόσο για τους χρήστες, όσο και για τους διαχειριστές (μηχανικούς, τεχνικούς κ.λπ.).
- Η αυστηρότητα των μηχανισμών ελέγχου πρόσβασης είναι αντίστοιχη της διαβάθμισης των δεδομένων.

4.2 Ρόλοι & Υπευθυνότητες

- Οι ιδιοκτήτες πληροφοριών φέρουν την ευθύνη για:
  - ο τον καθορισμό του ποιος πρέπει να έχει πρόσβαση στους πόρους τους.
  - ο τη διασφάλιση ότι οι πόροι τους προστατεύονται από μη-εξουσιοδοτημένη πρόσβαση.
  - ο την περιοδική αναθεώρηση των δικαιωμάτων πρόσβασης.
  - ο τη διασφάλιση ότι οι χρήστες έχουν την κατάλληλη κατάρτιση σχετικά με την ασφάλεια.
- Οι διαχειριστές φέρουν την ευθύνη για:

  ο την παροχή βοήθειας στους ιδιοκτήτες των πληροφοριών στον έλεγχο της πρόσβασης στους πόρους τους.
  - ο την άμεση αφαίρεση της πρόσβαση από ένα σύστημα όταν ζητείται.
  - ο την αναφορά οποιασδήποτε μη-εξουσιοδοτημένης πρόσβασης που ανακαλύπτουν.
- Οι χρήστες των πληροφοριακών Συστημάτων φέρουν την ευθύνη για:
  - ο την κατανόηση των πολιτικών και των διαδικασιών πρόσβασης στους πόρους της Εταιρείας.
  - ο την υποστήριξη των διαδικασιών της Εταιρείας σχετικά με την απόκτηση ή την αφαίρεση της πρόσβασής τους στους πληροφοριακούς πόρους.
  - ο την προστασία των διαπιστευτηρίων πρόσβασής τους (π.χ. κωδικούς πρόσβασης).
  - ο την πρόσβαση μόνο σε εκείνους τους πόρους για τους οποίους είναι εξουσιοδοτημένοι και τη χρήση των πληροφοριών σύμφωνα με τα εργασιακά καθήκοντα και την πολιτική της Εταιρείας.

  ο την άμεση αναφορά πιθανών παραβιάσεων αυτής της πολιτικής στον προϊστάμενό τους ή στο τμήμα Τεχνικής

  Υποστήριξης.
- Οι προϊστάμενοι φέρουν την ευθύνη για:
  - ο την υποστήριξη των διαδικασιών της Εταιρείας για απόκτηση και αφαίρεση της πρόσβασης των υπαλλήλων και των αναδόχων στους πόρους.
  - ο τη διασφάλιση ότι οι υπάλληλοί τους εξουσιοδοτούνται για να έχουν πρόσβαση στους πόρους που απαιτούνται για να εκτελέσουν τα καθήκοντά τους.
  - ο την ενημέρωση του Τμήματος Τεχνικής Υποστήριξης όταν δικαιώματα πρόσβασης ή λογαριασμοί πρόκειται να αφαιρεθούν.
  - ο την άμεση αναφορά πιθανών παραβιάσεων της παρούσας πολιτικής.

- Το τμήμα Ασφάλειας φέρει την ευθύνη για:
  - ο τη διεξαγωγή ελέγχων (auditing) για την διασφάλιση της συμμόρφωσης με τις διαδικασίες και τις οδηγίες που ορίζονται στην παρούσα πολιτική.
  - ο τη διασφάλιση ότι όλο το προσωπικό εκπαιδεύεται και ενημερώνεται για τις ευθύνες που αφορούν την ασφάλειας των υπολογιστών τους.
  - ο τη διασφάλιση ότι το προσωπικό IT και οι ανάδοχοι IT έχουν υποβληθεί στους κατάλληλους ελέγχους και κατάρτιση σχετικά με την ασφάλεια.

5.0 Αναθεώρηση και Αξιολόγηση

- Το τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

IX. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΡΟΣΩΠΙΚΟΥ (Personnel Security)

1.0 Εισαγωγή

Η μεγαλύτερη ζημιά / "διακοπή υπηρεσιών" σ' ένα σύστημα προέρχεται από ηθελημένες ή μη ενέργειες ατόμων. Οι χρήστες, οι υπεύθυνοι σχεδίασης, οι υπεύθυνοι υλοποίησης, οι διαχειριστές και τα διοικητικά στελέχη εμπλέκονται σε πολλά σημαντικά ζητήματα που αφορούν την ασφάλεια των πληροφοριών. Συνεπώς είναι σημαντικό να διασφαλιστεί:

- η εγκαθίδρυση ελέγχων για την πρόσβαση που παρέχεται στο προσωπικό,
- και η εφαρμογή διαδικασιών που ελαχιστοποιούν τους κινδύνους, σχετικούς με το προσωπικό, στους πόρους της Εταιρείας.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι να καθοριστούν οι διαδικασίες έγκρισης και διαχείρισης της πρόσβασης του προσωπικού στους πληροφοριακούς πόρους της Εταιρείας.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλους τους ιδιοκτήτες πληροφοριών, τους χρήστες πληροφοριών και τους υπεύθυνους Συστημάτων.

4.0 Πολιτική

4.1 Διαδικασίες & Οδηγίες

a) Οποιαδήποτε πρόσβαση χορηγείται στους πληροφοριακούς πόρους της Εταιρείας πρέπει να βασίζεται στις αρχές του "διαχωρισμού των καθηκόντων" και "ελάχιστων δικαιωμάτων" και να είναι σύμφωνη με τις πολιτικές και τις διαδικασίες ελέγχου πρόσβασης της Εταιρείας.

b) Οι χρήστες πληροφοριών πρέπει να έχουν κατάλληλη έγκριση για το επίπεδο ευαισθησίας των πόρων στους οποίους τους παρέχεται η πρόσβαση.

Πριν από τη χορήγηση πρόσβασης στις ευαίσθητες πληροφορίες, οι χρήστες πληροφοριών πρέπει να διαθέτουν την κατάλληλη έγκριση από τον αρμόδιο υπεύθυνο (δηλ, ιδιοκτήτη πληροφοριών) ή το τμήμα Ασφάλειας της Εταιρείας (για τους αναδόχους).

c) Το προσωπικό πρέπει να εκπαιδεύεται στις ευθύνες και τα καθήκοντα που αφορούν την ασφάλεια πληροφοριών και σχετίζονται με την εργασία του.

d) Πρέπει να υλοποιηθεί λεπτομερής διαδικασία για τη διαχείριση των λογαριασμών χρηστών, η οποία θα περιλαμβάνει την επεξεργασία των αιτημάτων για νέους λογαριασμούς, τη δημιουργία και διαγραφή των λογαριασμών καθώς και την παρακολούθηση των λογαριασμών και των εγκρίσεων της πρόσβασης χρηστών.

e) Πρέπει να υλοποιηθούν διαδικασίες για τους υπαλλήλους που αποχωρούν ή μμεταφέρονται. Ενδεικτικά και όχι περιοριστικά, οι διαδικασίες περιλαμβάνουν:

1) Αφαίρεση των δικαιωμάτων πρόσβασης και των λογαριασμών συστήματος

2) Επιστροφή οποιωνδήποτε πληροφοριακών πόρων της Εταιρείας (δεδομένα)

3) Διαδικασίες για τη μη φιλική λήξη που περιλαμβάνουν τη γρήγορη αφαίρεση της πρόσβασης Συστημάτων.

f) Οι ανάδοχοι πρέπει να υπογράφουν μια συμφωνία "μη-αποκάλυψης" που προστατεύει οποιαδήποτε ευαίσθητα δεδομένα στα οποία ο ανάδοχος χρειάζεται πρόσβαση.

4.2 Ρόλοι & Υπευθυνότητες

a) Οι ιδιοκτήτες πληροφοριών, για τους πόρους που ανήκουν στην κυριότητά τους, φέρουν την ευθύνη για τα ακόλουθα:

1) Τον καθορισμό του ποιος πρέπει να έχει πρόσβαση στους πόρους τους

2) Τον καθορισμό του επίπεδου ελέγχου που απαιτείται για την πρόσβαση

3) Τη διασφάλιση ότι οι πολιτικές και οι διαδικασίες ασφάλειας προσωπικού ακολουθούνται

b) Οι Υπεύθυνοι Συστημάτων φέρουν την ευθύνη για:

1) Την εφαρμογή των διαδικασιών της Εταιρείας για την παροχή ή την αφαίρεση της πρόσβασης στο προσωπικό για τους πόρους που αυτό διαχειρίζεται, συμπεριλαμβανομένης και της έγκαιρης διαγραφής ή απενεργοποίησης των λογαριασμών όταν τερματίζεται η απασχόληση των χρηστών.

2) Την εφαρμογή των αρχών "διαχωρισμού των καθηκόντων" και "ελάχιστων δικαιωμάτων" για τους πόρους που διαχειρίζονται.

3) Τον έλεγχο προς επαλήθευση ότι οι υπάλληλοι έχουν την κατάλληλη άδεια για τους πόρους στους οποίους τους

χορηγείται η πρόσβαση, σύμφωνα με τις απαιτήσεις άδειας που τίθενται από τους ιδιοκτήτες πληροφοριών.

c) Οι προϊστάμενοι πρέπει:

1) Να διαβιβάσουν στο προσωπικό τους τις απαιτήσεις ασφάλειας που περιγράφονται σ' αυτήν την πολιτική.

2) Να διασφαλίσουν ότι όλο το προσωπικό εκπαιδεύεται στις ευθύνες και τα καθήκοντα που αφορούν την ασφάλεια υπολογιστών και σχετίζονται με την εργασία του.

3) Να υποστηρίξουν τις πολιτικές και τις διαδικασίες της Εταιρείας για παροχή και αφαίρεση της πρόσβασης στους υπαλλήλους τους.

d) Οι χρήστες πληροφοριών πρέπει:

1) Να κατανοήσουν τις προσωπικές τους ευθύνες και καθήκοντα σχετικά με την ασφάλεια.

2) Να ακολουθούν τις διαδικασίες της Εταιρείας για την απόκτηση πρόσβασης στους πληροφοριακούς πόρους.

3) Να ενημερώνουν άμεσα τον ιδιοκτήτη πληροφοριών, τον υπεύθυνο Συστημάτων ή τον προϊστάμενό τους όταν δεν χρειάζονται πλέον την πρόσβαση σ' έναν πόρο.

e) Το τμήμα Ασφάλειας πρέπει:

1) Να εφαρμόζει διαδικασίες για να διασφαλίσει ότι η πρόσβαση στις πληροφορίες, μέσω των ΟΠΣ της Εταιρείας, ελέγχεται σύμφωνα με τις πολιτικές και τις διαδικασίες ασφάλειας της Εταιρείας.

2) Να παρακολουθεί την εμμονή στην πολιτική ασφάλειας προσωπικού.

5.0 Αναθεώρηση και Αξιολόγηση

- Το τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).

- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	Ημερομηνία	Αλλαγές
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

Χ. ΠΟΛΙΤΙΚΗ ΤΑΥΤΟΠΟΙΗΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗΣ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ

1.0 Εισαγωγή

Προκειμένου να διασφαλιστεί ότι τα μη εξουσιοδοτημένα άτομα δεν έχουν πρόσβαση στους ευαίσθητους πληροφοριακούς πόρους της Εταιρείας, είναι απαραίτητο αρχικά να εξακριβωθεί η ταυτότητα του χρήστη που προσπαθεί να αποκτήσει πρόσβαση στους πόρους. Οι μηχανισμοί ελέγχου πρόσβασης μπορούν στη συνέχεια να χρησιμοποιηθούν για να επιτρέψουν ή να περιορίσουν την πρόσβαση βάσει της εξακριβωμένης ταυτότητα χρήστη.
Η μέθοδος πιστοποίησης αυθεντικότητας που χρησιμοποιείται για κάθε σύστημα πρέπει να είναι ανάλογη του επιπέδου ευαισθησίας του συστήματος προς πρόσβαση (δηλ. τα πιο ευαίσθητα συστήματα πρέπει να χρησιμοποιήσουν τις ισχυρότερες μεθόδους πιστοποίησης αυθεντικότητας).

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι να χορηγηθεί η πρόσβαση στους πληροφοριακούς πόρους της Εταιρείας μόνο στους χρήστες για τους οποίους έχει προσδιοριστεί η ταυτότητα και πιστοποιηθεί η αυθεντικότητά τους (ταυτοποίηση και πιστοποίηση αυθεντικότητας). Η Εταιρεία πρέπει να εγκαθιδρύει τις διαδικασίες και τους ελέγχους για τη χορήγηση, την αλλαγή και τον τερματισμό της πρόσβασης στα πληροφοριακά συστήματα.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλα τα λειτουργικά ή υπό ανάπτυξη πληροφοριακά συστήματα που ανήκουν ή χρησιμοποιούνται από την Εταιρεία.

4.0 Πολιτική

4.1 Διαδικασίες & Οδηγίες

n) Κάθε σύστημα της Εταιρείας πρέπει να ενσωματώσει κατάλληλη ταυτοποίηση και πιστοποίηση αυθεντικότητας των χρηστών για να διασφαλιστεί ότι η πρόσβαση δεν χορηγείται σε μη εξουσιοδοτημένα άτομα. Οι χρήστες δεν θα έχουν πρόσβαση στους πληροφοριακούς πόρους της Εταιρείας χωρίς να έχει προηγηθεί η ταυτοποίηση και πιστοποίηση αυθεντικότητάς τους (δηλ. "συνδεμένος χρήστης" – "logging on").

o) Η Εταιρεία πρέπει να αναπτύξει και να ακολουθήσει λεπτομερείς διαδικασίες για τη δημιουργία, την αφαίρεση, και την τροποποίηση των λογαριασμών χρηστών και των διαπιστευτηρίων πιστοποίησης αυθεντικότητας.

p) Οι λογαριασμοί χρηστών πρέπει να ακολουθούν τις ακόλουθες οδηγίες:

1) Να επιτρέπεται μόνο ένας χρήστης ανά λογαριασμό. Η ταυτότητα χρήστη (user ID) δεν πρέπει ποτέ να διαμοιράζεται.

2) Να μην εγκαθίσταται ποτέ ένας guest/guest λογαριασμό. Πρέπει να γίνεται αφαίρεση οποιουδήποτε λογαριασμού "φιλοξενουμένων" – "guest" που δημιουργείται εξ' ορισμού από το σύστημα εκτός αν είναι απόλυτα αναγκαίος και εγκεκριμένος από το ιδιοκτήτη του συστήματος και το τμήμα Ασφάλειας.

3) Κανένας λογαριασμό δεν θα ονομαστεί με γενικά ονόματα τα οποία μπορεί κάποιος εύκολα να τα μαντέψει (όπως "anonymous", "guest", "admin", "ftp", "telnet", "www", "host", "user", "test", "bin", "nobody", κ.λπ...) εκτός αν είναι τεχνικά απολύτως αναγκαία για το σύστημα.

4) Οι εξ' ορισμού λογαριασμοί που είναι παρόντες κατά την αρχική εγκατάσταση του συστήματος πρέπει να αφαιρούνται ή να μετονομάζονται εκτός αν είναι τεχνικά απολύτως αναγκαίοι για το σύστημα.

5) Οι λογαριασμοί πρέπει να απενεργοποιούνται αμέσως με τη λήξη της συνεργασίας μ' ένα υπάλληλο ή ανάδοχο.

6) Οι λογαριασμοί που δεν χρησιμοποιούνται πρέπει να απενεργοποιούνται τουλάχιστον σε διμηνιαία βάση.

7) Οι λογαριασμοί για τους αναδόχους και τους προσωρινούς υπαλλήλους πρέπει να λήγουν κατά την ημερομηνία λήξης της σύμβασης τους.

q) Οι λογαριασμοί διαχειριστών πρέπει να ακολουθούν τις ακόλουθες οδηγίες:

1) Τα ονόματα των λογαριασμών διαχειριστών πρέπει να μετονομάζονται, εφόσον είναι εφικτό, για να καταστεί πιο δύσκολο στους επιτιθέμενους να μαντέψουν τα ονόματα αυτών των λογαριασμών.

2) Κάθε άτομο που έχει μια εύλογη ανάγκη να κάνει χρήση δικαιωμάτων διαχειριστή πρέπει να έχει δικό του λογαριασμό διαχειριστή, τον οποίο θα χρησιμοποιεί για να εκτελέσει τις διαχειριστικές λειτουργίες. Η χρήση του κύριου λογαριασμού διαχειριστή σε κάθε σύστημα πρέπει να περιορίζεται μόνον για έκτακτες ανάγκες καθώς και στο καθορισμένο προσωπικό για τη διαχείριση των πληροφοριακών πόρων. Αυτό προστατεύει τον κύριο λογαριασμό διαχειριστή και παρέχει τις απαραίτητες "εγγραφές ελέγχου" – "audit trails" των διαχειριστικών ενεργειών.

3) Όλοι οι λογαριασμοί με διαχειριστικά δικαιώματα πρέπει να έχουν ισχυρούς κωδικούς πρόσβασης ή άλλες εναλλακτικές ισχυρές μμεθόδους πιστοποίησης αυθεντικότητας.

r) Οι κωδικοί πρόσβασης που χρησιμοποιούνται για πιστοποίηση αυθεντικότητας πρέπει να ακολουθούν την "Πολιτική κωδικών πρόσβασης" της Εταιρείας.

s) Πληροφορίες διαπιστευτηρίων λογαριασμών (π.χ. ταυτότητες χρηστών - "IDs", κωδικοί πρόσβασης) που αποθηκεύονται στις συσκευές (όπως ο κωδικός πρόσβασης "enable" στα αρχεία διαμόρφωσης δρομολογητών) πρέπει να κρυπτογραφούνται.

t) Για την αποφυγή επιθέσεων "brute force", σε κάθε σύστημα πρέπει να ενεργοποιείται το προσωρινό κλείδωμα ενός λογαριασμού μετά από τρεις άκυρες προσπάθειες σύνδεσης. Η απενεργοποίηση του λογαριασμού πρέπει να γίνεται από έναν διαχειριστή ασφάλειας συστήματος.

u) Η Εταιρεία πρέπει να περιορίζει την πρόσβαση στα δεδομένα πιστοποίησης αυθεντικότητας. Τα δεδομένα πιστοποίησης αυθεντικότητας πρέπει να προστατεύονται με ελέγχους πρόσβασης και κρυπτογράφηση για να αποτραπεί η λήψη των δεδομένών από μη εξουσιοδοτημένα άτομα.

4.2 Ρόλοι & Υπευθυνότητες

f) Το προσωπικό πρέπει να κατανοήσει τις ευθύνες του για την προστασία των ταυτοτήτων χρηστών (user IDs) και των κωδικών πρόσβασης. Σε περίπτωση που κάποιο μέλος του προσωπικού αντιληφθεί ότι ένας κωδικός πρόσβασης ή κάποια άλλα διαπιστευτήρια Συστημάτων έχουν αποκαλυφθεί πρέπει να ειδοποιεί αμέσως έναν προϊστάμενο ή έναν υπεύθυνο Συστημάτων.

g) Οι προϊστάμενοι πρέπει να διασφαλίσουν ότι το προσωπικό τους:

- κατανοεί και συμμορφώνεται με τις οδηγίες που περιλαμβάνονται στην παρούσα πολιτική,
- ειδοποιεί αμέσως τους υπεύθυνους Συστημάτων για τους λογαριασμούς που πρέπει να απενεργοποιηθούν

ο αναφέρει οποιαδήποτε πιθανή παραβίαση ή αποκάλυψη των διαπιστευτηρίων στο τμήμα Ασφάλειας και τους

Υπεύθυνους Συστημάτων.

h) Οι Υπεύθυνοι Συστημάτων πρέπει να εφαρμόσουν τις κατάλληλες μεθόδους ταυτοποίησης και πιστοποίησης αυθεντικότητας για τους πληροφοριακούς πόρους στην περιοχή ευθύνης τους, να καθοδηγήσουν τους χρήστες ως προς τη χρήση τους και να αναφέρουν οποιαδήποτε παραβίαση στους πόρους αυτούς στο τμήμα Ασφάλειας και τον Ιδιοκτήτη Πληροφοριών.

i) Οι ιδιοκτήτες πληροφοριών πρέπει να διασφαλίσουν ότι οι κατάλληλες μέθοδοι ταυτοποίησης και πιστοποίησης αυθεντικότητας εφαρμόζονται για τους πόρους που τους ανήκουν, βάσει της κατηγοριοποίησης και το επίπεδο του κινδύνου που ορίζεται για τον πόρο.

j) Το τμήμα Ασφάλειας πρέπει να προετοιμάσει τις οδηγίες και τα πρότυπα για τα διαπιστευτήρια χρηστών, να διεξάγει τις αναθεωρήσεις συμμόρφωσης και να εγκρίνει την έκδοση των διαπιστευτηρίων διαχειριστών.

k) Οι υπεύθυνοι για την ανάπτυξη Συστημάτων πρέπει να διασφαλίσουν ότι τα συστήματα τους υποστηρίζουν τις διαδικασίες και τις οδηγίες που καθορίζονται στην παρούσα πολιτική.

5.0 Αναθεώρηση και Αξιολόγηση

- Το τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

XI. ΠΟΛΙΤΙΚΗ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

1.0 Εισαγωγή

Οι κωδικοί πρόσβασης (passwords) είναι μια από τις πιο σημαντικές συνιστώσες της ασφάλειας υπολογιστών. Αποτελούν την πρώτη γραμμή προστασίας για τους λογαριασμούς χρηστών (user accounts). Ένας κακώς επιλεγμένος κωδικός πρόσβασης εκθέτει την Εταιρεία στον κίνδυνο της πρόσβασης των Συστημάτων της από μη εξουσιοδοτημένα άτομα, με αποτέλεσμα να υπάρχει το ενδεχόμενο να παραβιαστούν και να τροποποιηθούν αυθαίρετα τα δεδομένα του συστήματος και να απειλείται η ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των πληροφοριών της.

2.0 Σκοπός

Ο σκοπός αυτής της πολιτικής είναι να καθιερωθούν πρότυπα για τη δημιουργία και την προστασία "ισχυρών" κωδικών πρόσβασης, καθώς και για τις διαδικασίες διαχείρισής τους.

3.0 Πεδίο εφαρμογής

Το πεδίο εφαρμογής αυτής της πολιτικής περιλαμβάνει όλα τα μέλη του προσωπικού που έχουν ή είναι υπεύθυνοι για κάποιο λογαριασμό σε οποιοδήποτε σύστημα/εφαρμογή στο δίκτυο της Εταιρείας.

4.0 Πολιτική

4.1 Οδηγίες δημιουργίας κωδικών πρόσβασης

Ο κωδικός πρόσβασης
πρέπει**:**

- να μην είναι λέξη που μπορεί να βρεθεί σε λεξικό αναζήτησης, να μην περιέχει ονόματα, ημερομηνίες, επαναλαμβανόμενους χαρακτήρες (aaabbb, qwerty, 123321, κ.λπ.)
- να περιέχει κεφαλαία και μικρά γράμματα, αριθμούς και ειδικούς χαρακτήρες (!@#$%&*()[]{}<>/?=+-\….)
- να περιέχει τουλάχιστον έναν αλφαβητικό χαρακτήρα και τουλάχιστον ένα ψηφίο ή ειδικό χαρακτήρα
- να έχει μήκος τουλάχιστον έξι (6) χαρακτήρες

4.2 Οδηγίες προστασίας κωδικών πρόσβασης

- Να μην αποκαλύπτεται σε τρίτους, έστω και εάν αυτοί είναι υπάλληλοι της Εταιρείας, ανώτερα διοικητικά στελέχη ή ακόμα και οι διαχειριστές (μηχανικοί) των πληροφοριακών Συστημάτων της Εταιρείας.
- Να μη σημειώνεται ούτε ηλεκτρονικά (π.χ. κινητά τηλέφωνα, σημειώσεις του outlook, κ.λπ.) ούτε χειρόγραφα, (π.χ. ατζέντες, ημερολόγια, post-it κ.λπ.).
- Οι χρήστες να μην αποκαλύπτουν τον κωδικό πρόσβασης σε συναδέλφους όταν πρόκειται να απουσιάσουν (πχ. λόγω αδείας ή ασθενείας).

- Οι κωδικοί πρόσβασης των διαχειριστών Συστημάτων/εφαρμογών που δεν κατέχουν πλέον τη συγκεκριμένη θέση πρέπει να αλλάζονται άμεσα.
- Οι Υπεύθυνοι Ασφάλειας Συστημάτων πρέπει να πραγματοποιούν ελέγχους για την ασφάλεια των κωδικών πρόσβασης.
- Να αλλαχτεί αμέσως αν υπάρχει η υπόνοια ότι έχει αποκαλυφθεί.
- Να αλλάζει τουλάχιστον κάθε 4 μήνες (120 ημέρες).
- Να είναι διαφορετικός από τον εξ' ορισμού (default) κωδικό (public, private, system) της υπηρεσίας που χρησιμοποιείται.
- Να μην αναφέρεται σε ερωτηματολόγια ή αναφορές ασφάλειας.

4.3 Κωδικοί πρόσβασης και ανάπτυξη εφαρμογών

Οι υπεύθυνοι για την ανάπτυξη εφαρμογών πρέπει να εξασφαλίσουν ότι τα προγράμματά τους περιέχουν τις ακόλουθες προφυλάξεις ασφάλειας.
Οι εφαρμογές:

- Πρέπει να υποστηρίζουν την πιστοποίηση αυθεντικότητας μεμονωμένων χρηστών και όχι ομάδων χρηστών,
- πρέπει να επιτρέπουν κάποιο είδος διαχείρισης ρόλων, έτσι ώστε ένας χρήστης να μπορεί να αναλάβει τις λειτουργίες ενός άλλου χρήστη, χωρίς να χρειάζεται να είναι γνωστός ο κωδικός πρόσβασής του,
- Πρέπει να υποστηρίζουν TACACS+, RADIUS με ανάκτηση ασφάλειας Actice Directory όπου αυτό είναι εφικτό,
- Δεν πρέπει να αποθηκεύουν τους κωδικούς πρόσβασης σε απλό κείμενο (plain text) ή με οποιαδήποτε εύκολα αντιστρέψιμή μμορφή.

4.4 Κωδικοί πρόσβασης και διαχειριστές Συστημάτων/εφαρμογών

Όπου είναι τεχνικά εφικτό θα πρέπει το σύστημα/εφαρμογή να τηρεί τους ακόλουθους κανόνες:

- Να εμποδίζει τους χρήστες να εισάγουν «κακώς επιλεγμένους» κωδικούς πρόσβασης που εύκολα μπορεί να αποκαλυφθούν ("aaabbb", "123456").
- Κάθε χρήστης να έχει τη δυνατότητα να αλλάζει τον κωδικό πρόσβασης.
- Μετά από τρεις "3" εσφαλμένες προσπάθειες εισαγωγής κωδικού πρόσβασης το σύστημα να κλειδώνει την δυνατότητα του χρήστη για περαιτέρω προσπάθειες πρόσβασης. Μόνο ο διαχειριστής του συστήματος θα πρέπει να έχει τη δυνατότητα να ξεκλειδώσει το λογαριασμό του χρήστη.
- Να ορίζει περίοδο αλλαγής κωδικού πρόσβασης. Η περίοδος αλλαγής για τους διαχειριστές Συστημάτων/εφαρμογών πρέπει να οριστεί στις "90" ημέρες και για τους χρήστες στις "120" ημέρες.
- Να ορίζει ελάχιστο μέγεθος κωδικού πρόσβασης. Το μέγεθος πρέπει να οριστεί σε τουλάχιστον "8" χαρακτήρες για τους διαχειριστές Συστημάτων/εφαρμογών και σε τουλάχιστον "6" χαρακτήρες για τους χρήστες.
- Να ορίζει αριθμό συνεχόμενων κωδικών πρόσβασης που δεν μπορούν να χρησιμοποιηθούν επειδή χρησιμοποιήθηκαν στο παρελθόν. Ο αριθμός αυτός πρέπει να οριστεί σε "3" συνεχόμενους κωδικούς πρόσβασης.
- Να αποθηκεύει τους κωδικούς πρόσβασης κωδικοποιημένους.
- Να υποχρεώνει την αλλαγή κωδικού πρόσβασης μετά την πρώτη πρόσβαση του χρήστη στο σύστημα.

- Να γίνεται καταγραφή αλλαγών των κωδικών πρόσβασης στους πίνακες του συστήματος.
- Να λαμβάνει επιπλέον μέτρα προστασίας για τη χρήση των κωδικών πρόσβασης από απόσταση (πχ. κρυπτογραφημένα κανάλια επικοινωνίας).
- Η χρήση κωδικών πρόσβασης από απόσταση σε εφαρμογές θα γίνεται μόνον αφού έχει προηγηθεί η διαδικασία αποτίμησης κινδύνου.

5.0 Αναθεώρηση και Αξιολόγηση

- Το τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν την βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	Ημερομηνία	Αλλαγές
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

ΧΙΙ. ΠΟΛΙΤΙΚΗ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΛΟΓΙΚΗΣ ΠΡΟΣΒΑΣΗΣ

1.0 Εισαγωγή

Η υπηρεσία απομακρυσμένης λογικής πρόσβασης παρέχει σύνδεση στο δίκτυο της Εταιρείας μέσω ενός, μη ελεγχόμενου από την Εταιρεία, δικτύου, συσκευής ή μέσου. Χρησιμοποιώντας την υπηρεσία απομακρυσμένης λογικής πρόσβασης, οι εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο, τις υπηρεσίες αρχείων, τις επιχειρησιακές εφαρμογές και τις IP-βασισμένες υπηρεσίες της Εταιρείας, εφόσον μπορούν να παρασχεθούν.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι να καθοριστούν τα πρότυπα για την απομακρυσμένη σύνδεση οποιουδήποτε Η/Υ με τα ΟΠΣ της Allweb Solutions S.A.. Αυτά τα πρότυπα έχουν ως σκοπό να ελαχιστοποιήσουν την πιθανή έκθεση της Εταιρείας σε ζημιές που μπορούν να προκύψουν από την μη-εξουσιοδοτημένη χρήση των πόρων του. Οι ζημιές περιλαμβάνουν την απώλεια ευαίσθητων ή εμπιστευτικών δεδομένων, πνευματικής ιδιοκτησίας, ζημίας στη δημόσια εικόνα, ζημίας σε κρίσιμα εσωτερικά συστήματα της Allweb Solutions S.A.,κ.λπ.

3.0 Πεδίο Εφαρμογής

Η πολιτική αυτή ισχύει για όλο το προσωπικό της Εταιρείας, τους αναδόχους και προμηθευτές που χρησιμοποιούν εταιρικό ή ιδιόκτητο Η/Υ για να συνδεθούν στο δίκτυο της Allweb Solutions S.A. Η πολιτική αυτή ισχύει για τις συνδέσεις απομακρυσμένης πρόσβασης που χρησιμοποιούνται για την εκτέλεση εργασίας για λογαριασμό της Εταιρείας.

4.0 Πολιτική

1. Η Εταιρεία οφείλει να εξασφαλίζει ότι για την απομακρυσμένη πρόσβαση εργαζομένων και συνεργατών στο δίκτυο της, δίνεται η ίδια σημασία με την τοπική σύνδεση του χρήστη, καθώς και ότι η πρόσβαση του χρήστη θα πρέπει να περιορίζεται στις περιπτώσεις που αυτό είναι αναγκαίο για τις επιχειρησιακές του ανάγκες.
2. Η υπηρεσία απομακρυσμένης λογικής πρόσβασης παρέχεται από την Διεύθυνση Πληροφορικής (οι πύλες της υπηρεσίας εγκαθιδρύονται και ρυθμίζονται από το τμήμα Τεχνικής Υποστήριξης). Σε κανένα άλλο τμήμα δεν επιτρέπεται να υλοποιήσει υπηρεσίες αυτής.
3. Όλη η δικτυακή δραστηριότητα, κατά τη διάρκεια μιας συνόδου απομακρυσμένης πρόσβασης, υπόκειται στις

   Πολιτικές Ασφάλειας της Εταιρείας και μπορεί να καταγράφεται.

4. Η απομακρυσμένη πρόσβαση ελέγχεται με τη χρήση κωδικού πρόσβασης. Για περισσότερες λεπτομέρειες συμβουλευτείτε το έγγραφο "Πολιτική Κωδικών Πρόσβασης".
5. Η απομακρυσμένη πρόσβαση πραγματοποιείται με χρήση μηχανισμών ασφαλούς αυθεντικοποίησης και κρυπτογράφησης (π.χ. μέσω VPN)

6. Οι υπάλληλοι και οι ανάδοχοι της Εταιρείας με προνόμια απομακρυσμένης πρόσβασης πρέπει να εξασφαλίσουν ότι ο προσωπικός Η/Υ, με τον οποίο συνδέονται στο εταιρικό δίκτυο της Allweb Solutions S.A από απόσταση, δε συνδέεται συγχρόνως με οποιοδήποτε άλλο δίκτυο.
7. Οι χρήστες απομακρυσμένης πρόσβασης θα αποσυνδέονται αυτόματα από το εταιρικό δίκτυο της Allweb Solutions S.A μετά από τριάντα λεπτά αδράνειας. Τα "Pings" ή άλλες τεχνητές διαδικασίες δικτύων δε μπορούν να χρησιμοποιηθούν για να κρατήσουν τη σύνδεση ανοικτή.
8. Η Εταιρεία οφείλει να εξασφαλίζει ότι η απομακρυσμένη πρόσβαση συνεργατών θα πρέπει να επιτρέπεται μόνο για συγκεκριμένο χρονικό διάστημα και να γίνεται είτε με την χρήση κωδικών μιας πρόσβασης είτε με την απενεργοποίηση των λογαριασμών μετά το πέρας του διαστήματος αυτού. Τουλάχιστον κάθε τρεις μήνες θα πρέπει να ελέγχεται η υλοποίηση των απαιτούμενων μεταβολών των κωδικών και η απενεργοποίηση των λογαριασμών.
9. Η Εταιρεία οφείλει να εξασφαλίζει ότι η απομακρυσμένη πρόσβαση συνεργατών θα επιτρέπεται μόνο μετά από έγκριση σχετικών αιτημάτων, όπου θα αναγράφεται ο λόγος της πρόσβασης, το σύστημα στο οποίο θα πραγματοποιηθεί η πρόσβαση καθώς και το χρονικό διάστημα που απαιτείται.
10. Ο προσωπικός τεχνικός εξοπλισμός του χρήστη της υπηρεσίας, αποτελεί μια de facto επέκταση του εταιρικού δικτύου, και ως τέτοιος υπόκειται στις Πολιτικές Ασφάλειας της Allweb Solutions S.A..
11. Η εταιρεία οφείλει να διατηρεί αρχείο στο οποίο θα καταγράφονται τα στοιχεία χρηστών απομακρυσμένης πρόσβασης (εργαζόμενοι, συνεργάτες) καθώς και τα δικαιώματα πρόσβασης τους. Τουλάχιστον κάθε τρεις μήνες θα πρέπει να ελέγχεται η αντιστοίχιση των λογαριασμών απομακρυσμένης πρόσβασης και των στοιχείων του αρχείου αυτού.
12. Η εταιρεία οφείλει να διατηρεί αρχείο στο οποίο θα καταγράφονται για εργαζόμενους και συνεργάτες τα ΟΠΣ στα οποία επιτρέπεται η απομακρυσμένη πρόσβαση καθώς και οι τεχνικοί τρόποι απομακρυσμένης πρόσβασης.
    Για το συγκεκριμένο αρχείο πρέπει να καταγραφεί και υλοποιηθεί διαδικασία διαχείρισης των λογαριασμών.

5.0 Αναθεώρηση και Αξιολόγηση

- Το τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν την βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	Ημερομηνία	Αλλαγές
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

XIII. ΠΟΛΙΤΙΚΗ ΙΔΕΑΤΩΝ ΙΔΙΩΤΙΚΩΝ ΔΙΚΤΥΩΝ (Virtual Private Network - VPN)

1.0 Εισαγωγή

Ένα "Ιδεατό Ιδιωτικό Δίκτυο" (VPN) παρέχει σε απομακρυσμένα δίκτυα ή σε μεμονωμένους χρήστες ασφαλή πρόσβαση στο δίκτυο της Εταιρείας, κάνοντας χρήση ενός δημοσίου δικτύου τηλεπικοινωνιών, όπως το Διαδίκτυο. Η επικοινωνία σ' ένα VPN δίκτυο προστατεύεται από μηχανισμούς κρυπτογράφησης και πιστοποίησης αυθεντικότητας.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι να οριστούν οι κανόνες ασφάλειας για τις συνδέσεις απομακρυσμένης πρόσβασης, με τη χρήση Ιδεατών Ιδιωτικών Δικτύων (VPN), στο εταιρικό δίκτυο της Allweb Solutions S.A..

3.0 Πεδίο εφαρμογής

Αυτή η πολιτική ισχύει για όλο το προσωπικό της Εταιρείας, τους αναδόχους, πελάτες και προμηθευτές που χρησιμοποιούν το VPN για να έχουν πρόσβαση στο εταιρικό δίκτυο της Allweb Solutions. Αυτή η πολιτική ισχύει για υλοποιήσεις VPN που κατευθύνονται μέσω ενός IPSec Concentrator.

4.0 Πολιτική

- Εγκεκριμένο προσωπικό της Allweb Solutions S.A. και εξουσιοδοτημένοι τρίτοι (πελάτες, προμηθευτές, κ.λπ.) μπορούν να χρησιμοποιήσουν την υπηρεσία VPN, η οποία αποτελεί "υπηρεσία διαχειριζόμενη από το χρήστη". Αυτό σημαίνει ότι ο χρήστης είναι υπεύθυνος για την επιλογή φορέα παροχής υπηρεσιών Διαδικτύου (ISP), το συντονισμό της εγκατάστασης, την εγκατάσταση του απαραίτητου λογισμικού και την καταβολή σχετικών τελών.
- Η πρόσβαση VPN παρέχεται από τη Διεύθυνση Πληροφορικής. Οι πύλες VPN εγκαθίστανται και ρυθμίζονται από το τμήμα Τεχνικής Υποστήριξης. Κανένα άλλο τμήμα δεν μμπορεί να υλοποιήσει υπηρεσίες VPN.
- Μόνο εγκεκριμένο λογισμικό VPN client, το οποίο υποστηρίζεται από το τμήμα δικτύων, μπορεί να χρησιμοποιηθεί.
- Όλη η δικτυακή δραστηριότητα, κατά τη διάρκεια μιας VPN συνόδου, υπόκειται στις Πολιτικές Ασφάλειας της Εταιρείας και μπορεί να καταγράφεται.
- Είναι ευθύνη των υπαλλήλων με προνόμια VPN να διασφαλίσουν ότι δε θα επιτραπεί η πρόσβαση στα εσωτερικά δίκτυα της Εταιρείας σε μη εξουσιοδοτημένους χρήστες.
- Η VPN πρόσβαση ελέγχεται με τη χρήση κωδικού πρόσβασης. Για περισσότερες λεπτομέρειες ανατρέξτε στο έγγραφο "Πολιτική Κωδικών Πρόσβασης".
- Όταν οι χρήστες συνδέονται ενεργά με το εταιρικό δίκτυο, τα VPNs θα αναγκάζουν όλη την κυκλοφορία από και προς τον Η/Υ να περνά πάνω από το VPN tunnel.
- Δεν επιτρέπεται το διπλό tunneling (Dual "split" tunneling): επιτρέπεται μόνον μια σύνδεση δικτύου.

- Οι χρήστες VPN θα αποσυνδέονται αυτόματα από το εταιρικό δίκτυο της Allweb Solutions μετά από τριάντα λεπτά αδράνειας. Τα "Pings" ή άλλες τεχνητές διαδικασίες δικτύων δεν μπορούν να χρησιμοποιηθούν για να κρατήσουν τη σύνδεση ανοικτή.
- Ο VPN concentrator περιορίζεται σε έναν απόλυτο χρόνο σύνδεσης 24 ωρών.

- Ο προσωπικός τεχνικός εξοπλισμός του VPN χρήστη, αποτελεί μια de facto επέκταση του εταιρικού δικτύου της Allweb Solutions S.A, και ως τέτοιος υπόκειται στις Πολιτικές Ασφάλειας της Εταιρείας.

5.0 Αναθεώρηση και Αξιολόγηση

- Το τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν την βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

XIV. ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΗΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

1.0 Εισαγωγή

Τα σύγχρονα Πληροφοριακά Συστήματα είναι σύνθετα και αποτελούνται από πολλά αλληλεξαρτώμενα και διασυνδεμένα στοιχεία. Η πολιτική αυτή καθορίζει τον τρόπο με τον οποίο η Εταιρεία εγκαταστεί και διαχειρίζεται το Πληροφοριακό της Σύστημα ώστε να συμβάλει στη διασφάλιση του απορρήτου των επικοινωνιών.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι να προσδιορίσει τις απαιτήσεις που πρέπει να ικανοποιούνται κατά τη διάρκεια ζωής του Πληροφοριακού Συστήματος προκειμένου να διασφαλίζεται το απόρρητο των επικοινωνιών.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλα τα συστήματα, δίκτυα, εφαρμογές και λοιπούς πληροφοριακούς πόρους που ανήκουν ή χρησιμοποιούνται από την Εταιρεία.

4.0 Πολιτική

4.1 Γενικές Αρχές

- Η εταιρεία οφείλει να λαμβάνει όλα τα απαραίτητα μέτρα προκειμένου να ελαχιστοποιείται ο κίνδυνος διαρροής πληροφοριών που σχετίζονται με το απόρρητο των επικοινωνιών των συνδρομητών ή χρηστών των παρεχόμενων υπηρεσιών.
- Η εταιρεία οφείλει να διατηρεί αρχείο στο οποίο, για οποιαδήποτε αλλαγή ή συμβάν στο Πληροφοριακό Σύστημα (λειτουργικό σύστημα και εφαρμογές), να καταγράφεται η ημερομηνία, ο τρόπος, η αιτιολόγηση και ο εργαζόμενος που πραγματοποίησε την αλλαγή.
- Το αρχείο πρέπει να ενημερώνεται και να διατηρείται από συγκεκριμένη διοικητική οντότητα ή εργαζόμενο της εταιρείας.

4.2 Διαδικασίες και Οδηγίες

Η εταιρεία οφείλει να διατηρεί και να εφαρμόζει διαδικασίες για τα παρακάτω στάδια Διαχείρισης και Εγκατάστασης του Πληροφοριακού Συστήματος με σκοπό τη διασφάλιση του απορρήτου των επικοινωνιών.

1) Προμήθεια Υλικού και Λογισμικού.
   - Συντάσσεται κατάλογος απαιτήσεων που αφορούν ρυθμίσεις ή χαρακτηριστικά του υπό προμήθεια υλικού/λογισμικού.
   - Θα πρέπει οι απαιτήσεις να συμμορφώνονται με τις προδιαγραφές ασφάλειας όπως καθορίζονται στα αποτελέσματα της αποτίμησης κινδύνου.
2) Εγκατάσταση , Δοκιμή , Αποδοχή , Λειτουργία , Έλεγχος ορθής λειτουργίας Υλικού και Λογισμικού
   - Πραγματοποίηση δοκιμών, παρακολούθηση ορθής λειτουργίας σύμφωνα με τις καταγεγραμμένες απαιτήσεις και καταγραφή αποτελεσμάτων.

- Σύνταξη, υπογραφή από τα εμπλεκόμενα μέρη και καταχώρηση σε αρχείο έκθεση αποδοχής του ΟΠΣ αφού ολοκληρωθεί με επιτυχία η δοκιμαστική λειτουργία

3) Συντήρηση – Υποστήριξη -Λειτουργία Υλικού και Λογισμικού.

- Πρέπει να διατηρείται αρχείο με τις ενέργειες που αφορούν το λειτουργικό σύστημα και τις εφαρμογές.
- Οι διαδικασίες ελέγχου (Συντήρηση – Υποστήριξη -Λειτουργία Υλικού και Λογισμικού) μεταξύ άλλων πρέπει να περιλαμβάνουν την παρακολούθηση της ορθής λειτουργίας των ΟΠΣ, μέσω του ελέγχου συμβάντων και των συναγερμών κάθε συστήματος, ώστε να εμποδίζονται τυχόν σφάλματα ή κενά ασφάλειας.

4) Διαγραφή-Απόσυρση Υλικού και Λογισμικού.

- Πρέπει ναδιατηρείται αρχείο με δεδομένα του Πληροφοριακού Συστήματος που διαγράφονται καθώς και το όνομα του εργαζομένου που υλοποιεί την ενέργεια.
- Πρέπει να ορίζονται ενέργειες ώστε να διασφαλίζεται, σύμφωνα με την νομοθεσία, ότι όταν διαγράφεται και αποσύρεται υλικό ή λογισμικό, η πληροφορία που έχει εγγραφεί στον εξοπλισμό του διαγράφεται οριστικά και δεν μπορεί να χρησιμοποιηθεί από τρίτους.

5.0 Αναθεώρηση και Αξιολόγηση

- Το τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

XV. ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

1.0 Εισαγωγή

Σύμφωνα με την Ελληνική και Ευρωπαϊκή Νομοθεσία που αφορά τις ηλεκτρονικές επικοινωνίες, η Εταιρεία οφείλει να διαθέτει σαφή Διαδικασία Χειρισμού Περαστικών Ασφάλειας, τα οποία απειλούν την ασφάλεια των επικοινωνιακών υποδομών αλλά και τη διασφάλιση του απορρήτου των επικοινωνιών που διεξάγονται μέσω του παρόχου.
Η ύπαρξη μιας επίσημα τεκμηριωμένης και σαφώς κατανοητής διαδικασίας χειρισμού περιστατικών ασφάλειας θα καταστήσει εφικτή τη γρήγορη και αποτελεσματική ανταπόκριση της Εταιρείας σε καταστάσεις που μπορούν να θέσουν σε κίνδυνο τους πληροφοριακούς της πόρους.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι να διασφαλιστεί ότι η Εταιρεία είναι σε θέση να αντιμετωπίσει τα σχετικά με την ασφάλεια υπολογιστών περιστατικά με τέτοιο τρόπο που να προστατεύει τις πληροφορίες της και να βοηθά στην προστασία των πληροφοριών άλλων που μπορεί να επηρεαστούν από το περιστατικό.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλους τους χρήστες, διαχειριστές και υπεύθυνους Συστημάτων της Εταιρείας.

4.0 Πολιτική

4.1 Διαδικασίες & Οδηγίες

- Όλα τα αναφερόμενα περιστατικά ασφάλειας θα αντιμετωπίζονται άμεσα και σύμφωνα με τις διαδικασίες χειρισμού περιστατικών ασφάλειας που ορίζει το τμήμα Ασφάλειας της Εταιρείας.
- Η Εταιρεία οφείλει να δημιουργήσει "Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας" και να καθιερώσει διαδικασίες αντιμετώπισης περιστατικών ασφάλειας πληροφοριών που θα εξετάζουν τα περιστατικά ασφάλειας υπολογιστών, συμπεριλαμβανομένης της κλοπής, της κακής χρήσης των δεδομένων, των εισβολών και του κακόβουλου λογισμικού. Οι διαδικασίες ενδεικτικά θα πρέπει να περιλαμβάνουν τα ακόλουθα:
    1. Στη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας πρέπει να υλοποιούνται οι παρακάτω ενέργειες:
        - Λεπτομερής καταγραφή κάθε περιστατικού ασφάλειας
            - Ημερομηνία, ώρα εκδήλωσης και περιγραφή του περιστατικού
            - Ημερομηνία και ώρα που έγινε αντιληπτό το περιστατικό από την εταιρεία

- Σημείο στο οποίο εκδηλώθηκε το περιστατικό (σύστημα, υπηρεσία, εφαρμογή, πρωτόκολλα, κ.α.)
- Συλλεχθέντα στοιχεία από την εταιρεία για τη διερεύνηση του περιστατικού (αρχεία καταγραφής, στοιχεία παραβίασης, κ.α.)

- Ενημέρωση για την ενδεχόμενη εμφάνιση του περιστατικού περισσότερες φορές
- Ενδεχόμενες συστάσεις σε θιγόμενα άτομα που επηρεάστηκαν από το περιστατικό

- Διερεύνηση των αιτιών και προσδιορισμός τεχνικών ή/και οργανωτικών αδυναμιών στις οποίες ενδεχομένως οφείλεται το περιστατικό ασφάλειας
- Καθορισμός των συνεπειών (αριθμός χρηστών που επηρεάστηκαν, τύπος και όγκος των δεδομένων που επηρεάστηκαν, κ.α) και υλοποίηση ενεργειών αποκατάστασης με συγκεκριμένο χρονοδιάγραμμα
- Ενημέρωση αρμόδιων στελεχών της εταιρείας, καθώς και θιγόμενων χρηστών των παρεχόμενων δικτύων ή υπηρεσιών
- Σύνταξη και διατήρηση σε αρχείο όλων των εγγράφων που σχετίζονται με τα περιστατικά ασφάλειας, από τα οποία θα τεκμηριώνεται και η εκτέλεση των αντίστοιχων προβλεπόμενων ενεργειών

2. Η εταιρεία οφείλει να δώσει υψηλή προτεραιότητα στο χειρισμό κρίσιμων περιστατικών για να παρεμποδιστεί η περαιτέρω ζημιά στους πληροφοριακούς πόρους της Εταιρείας.
3. Η εταιρεία οφείλει να παρέχει στους χρήστες των δικτύων ή υπηρεσιών του την δυνατότητα να καταγγέλλουν μα απλά μέσα την ενδεχόμενη παραβίαση του απορρήτου των επικοινωνιών τους.

4.2 Ρόλοι & Υπευθυνότητες

a) Το τμήμα Ασφάλειας φέρει την ευθύνη για:

1) την κατάρτιση και εφαρμογή οδηγιών πολιτικής για την αντιμετώπιση περιστατικών ασφάλειας υπολογιστών,

2) την ανάπτυξη διαδικασιών αντιμετώπισης περιστατικών,

3) τη συνεργασία με τους χρήστες, τους ιδιοκτήτες πληροφοριών και τους διαχειριστές Συστημάτων για τη διατύπωση και την υλοποίηση ενός σχεδίου δράσης,

4) την ενημέρωση των ιδιοκτητών πληροφοριών και της διοίκησης της Εταιρείας για σημαντικά περιστατικά και το σχέδιο δράσης,

5) τη διασφάλιση ότι όλα τα συμβάντα και οι ενέργειες επίλυσής τους είναι πλήρως τεκμηριωμένα,

6) τη διεξαγωγή ελέγχων ανά τακτά χρονικά διαστήματα ώστε να διασφαλιστεί η ετοιμότητα ενεργοποίησης όλων των μμηχανισμών και προσώπων που περιγράφονται στην παρούσα πολιτική.

b) Οι χρήστες των πληροφοριακών Συστημάτων φέρουν την ευθύνη για:

1) να πράξουν τα ακόλουθα εάν υποψιάζονται ότι ένα συμβάν ασφάλειας έχει εμφανιστεί:

ο να κατανοήσουν και να συμμορφωθούν με τις διαδικασίες αντιμετώπισης περιστατικών ασφάλειας της Εταιρείας,

ο να τεκμηριώσουν όλες τις σχετικές πληροφορίες για το πιθανό συμβάν,

ο να μοιραστούν τις υποψίες και τις πληροφορίες με το διευθυντή τους ή/και το τμήμα Ασφάλειας

ο να συνεργάζονται πλήρως και να βοηθάνε το τμήμα Ασφάλειας, τους διαχειριστές Συστημάτων και άλλο υπεύθυνο προσωπικό με την επίλυση του συμβάντος, όπως αυτό ζητείται.

c) Οι προϊστάμενοι φέρουν την ευθύνη για:

1) τη διασφάλιση ότι οι υπάλληλοί τους καταλαβαίνουν την πολιτική και τις διαδικασίες αντιμετώπισης περιστατικών ασφάλειας της Εταιρείας,

2) την ενημέρωση του Τμήματος Ασφάλειας σε διάστημα μιας εργάσιμής ημέρας μετά από το περιστατικό,

3) την παροχή σχετικών πληροφοριών με το περιστατικό στο τμήμα Ασφάλειας, όταν αυτό ζητηθεί.

d) Οι ιδιοκτήτες πληροφοριών φέρουν την ευθύνη για:

1) τη διασφάλιση ότι οι διαδικασίες αντιμετώπισης περιστατικών ασφάλειας είναι σε ισχύ για τους πόρους τους

2) την πληροφόρηση της διοίκησης της Εταιρείας για σημαντικά περιστατικά (σημαντική παραβίαση/έκθεση των δεδομένων, άρνηση της υπηρεσίας)

3) παρακολούθηση των περιστατικών για να διασφαλιστεί ότι τα γεγονότα έχουν επιλυθεί.

e) Οι διαχειριστές Συστημάτων φέρουν την ευθύνη για:

1) την παροχή βοήθειας στην αξιολόγηση του περιστατικού και το μμετριασμό του κινδύνου,

2) τη συνεργασία με το τμήμα Ασφάλειας, τους ιδιοκτήτες των Συστημάτων ή/και τους χρήστες για τη διατύπωση και εφαρμογή ενός σχεδίου δράσης,

3) την τεκμηρίωση και αναφορά των βημάτων που ελήφθησαν για το χειρισμό του περιστατικού στο Τμήμα

Ασφάλειας.

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

XVI. ΠΟΛΙΤΙΚΗ ΑΝΑΦΟΡΩΝ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ (Security Incident Reporting)

1.0 Εισαγωγή

Η διατήρηση της ασφάλειας των πληροφοριακών πόρων της Εταιρείας απαιτεί τη συνεργασία και τη συμμετοχή όλων. Είναι σημαντικό όλοι οι χρήστες πληροφοριών να βρίσκονται σε εγρήγορση σχετικά με την ασφάλεια των πληροφοριών και να αναφέρουν άμεσα οποιαδήποτε πιθανά περιστατικά προκειμένου να ελαχιστοποιηθεί η πιθανή ζημιά στην Εταιρεία.
Η πολιτική και οι διαδικασίες αναφοράς περιστατικών ασφάλειας της Εταιρείας επιτρέπουν στην Εταιρεία:

- γρήγορη και αποτελεσματική ανάκαμψη από τα περιστατικά ασφάλειας,
- απόκριση κατά τρόπο συστηματικό στα περιστατικά και ολοκλήρωση όλων των απαραίτητων βημάτων για το σωστό χειρισμό των περιστατικών,
- αποτροπή ή ελαχιστοποίηση της διάσπασης των κρίσιμων υπηρεσιών,
- και ελαχιστοποίηση της απώλειας ή της κλοπής των ευαίσθητων ή κρίσιμων πληροφοριών.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι ο καθορισμός των διαδικασιών αναφοράς περιστατικών ασφάλειας της Εταιρείας βάσει των οποίων όλοι οι χρήστες πληροφοριών της Εταιρείας πρέπει να αναφέρουν οποιαδήποτε πιθανά περιστατικά ασφάλειας πληροφοριών.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλους τους χρήστες των πληροφοριακών πόρων της Εταιρείας.

4.0 Πολιτική

4.1 Διαδικασίες & Οδηγίες

a) Όλα τα πιθανά περιστατικά ασφάλειας πρέπει να αναφέρονται άμεσα στο Τμήμα Ασφάλειας.

1) Ενδεικτικά και όχι περιοριστικά, τα περιστατικά περιλαμβάνουν:

- Πιθανές παραβιάσεις οποιασδήποτε πολιτικής ασφάλειας πληροφοριών της Εταιρείας.
- Απώλεια ή κλοπή φορητών υπολογιστών, κινητών συσκευών (όπως PDAs), security tokens ή άλλων στοιχείων που μπορούν να παρέχουν πρόσβαση στους πληροφοριακούς πόρους της Εταιρείας.
- Προσπάθειες από μη-εξουσιοδοτημένο εξωτερικό προσωπικό να αποκτήσει πρόσβαση στις πληροφορίες ή τα συστήματα της Εταιρείας.
- Τυχαία αποκάλυψη, τροποποίηση ή καταστροφή των πληροφοριών.

b) Όλα τα περιστατικά που αναφέρονται θα αντιμετωπίζονται σύμφωνα με τις πολιτικές και τις διαδικασίες Διαχείρισης

Περιστατικών Ασφάλειας της Εταιρείας.

1) Για κάθε περιστατικό πρέπει να συμπληρώνεται και να υποβάλλεται ένα έντυπο αναφοράς περιστατικού της Εταιρείας.

4.2 Ρόλοι & Υπευθυνότητες

a) Οι χρήστες πληροφοριών φέρουν την ευθύνη για την άμεση αναφορά των πιθανών περιστατικών στο Τμήμα Ασφάλειας ή στον ιδιοκτήτη των πληροφοριών κάνοντας χρήση των διαδικασιών αναφοράς περιστατικών ασφάλειας της Εταιρείας.

b) Οι προϊστάμενοι φέρουν την ευθύνη για τη διασφάλιση ότι οι υπάλληλοί τους καταλαβαίνουν και υποστηρίζουν τις πολιτικές και διαδικασίες αναφοράς περιστατικών ασφάλειας καθώς και για τη διασφάλιση ότι τα περιστατικά ασφάλειας αναφέρονται όσο το δυνατόν γρηγορότερα.

c) Το Τμήμα Ασφάλειας φέρει την ευθύνη για:

1) Την ανάπτυξη και διατήρηση των διαδικασιών αναφοράς και αντιμετώπισης των περιστατικών ασφάλειας.

2) Την έρευνα, τεκμηρίωση, επίλυση και παρακολούθηση των αναφερόμενων περιστατικών.

3) Την υποβολή εκθέσεων για τα περιστατικά στη διοίκηση και τις κατάλληλες εξωτερικές οντότητες (ΑΔΑΕ).

4) Τον καθορισμό του εάν απαιτείται επιπλέον παρακολούθηση του περιστατικού (follow up).

d) Οι υπεύθυνοι Συστημάτων φέρουν την ευθύνη για:

1) Την αναφορά οποιουδήποτε περιστατικού που αντιμετωπίζουν στο Τμήμα Ασφάλειας.

2) Την έρευνα και επίλυση των περιστατικών μέσα στο διαχειριστικό τομέα τους.

3) Την παροχή τεκμηρίωσης των περιστατικών και των μέτρων που έλαβαν για να τα επιλύσουν στο Τμήμα Ασφάλειας.

4) Την πλήρη συνεργασία με το Τμήμα Ασφάλειας, και την παροχή βοήθειας προς αυτό, για το χειρισμό του περιστατικού, όπως αυτό ζητείται.

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	Ημερομηνία	Αλλαγές
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

XVII. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ

1.0 Εισαγωγή

Οποιαδήποτε σύνδεση με συστήματα ή οργανισμούς εντός ή εκτός της Εταιρείας παρέχει ένα «άνοιγμα» σε μη-εξουσιοδοτημένα άτομα να αποκτήσουν πρόσβαση ή να επέμβουν στους πληροφοριακούς πόρους της Εταιρείας. Το εύρος των απειλών εκτείνεται από τους εισβολείς που παραβιάζουν το δίκτυο της Εταιρείας για να κλέψουν ή να τροποποιήσουν δεδομένα μέχρι τη διάσπαση υπηρεσιών που μπορεί να διαδοθεί από άλλα συστήματα. Για την αποτροπή, ανίχνευση και επίλυση των περιστατικών που προκύπτουν από αυτές τις απειλές, η Εταιρεία πρέπει να εφαρμόζει αντίστοιχα μέτρα προστασίας, όπως λύσεις Συστημάτων Firewall, ανίχνευσης εισβολών (IDS) καθώς και άλλων προφυλάξεων.

2.0 Σκοπός

Σκοπός της Πολιτικής Ασφάλειας Δικτύου είναι η εταιρεία να υλοποιήσει έναν λογικό διαχωρισμό των εσωτερικών της δικτύων από τα εξωτερικά δίκτυα και να διαμερίσει τα δίκτυα της σε ζώνες ασφάλειας ή υποδίκτυα, ανάλογα με το επίπεδο ασφάλειας που απαιτείται, με στόχο την απομόνωση σε ζώνες ασφάλειας, τον διαχωρισμό αυτών σε δικτυακό επίπεδο καθώς και τον έλεγχο της επικοινωνίας μεταξύ αυτών.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλο τον ενεργό εξοπλισμό δικτύων της Εταιρείας.

4.0Πολιτική

4.1 Διαδικασίες & Οδηγίες

a) Η Εταιρεία πρέπει να καταρτίζει και να διατηρεί ενημερωμένο αρχείο, στο οποίο περιγράφεται ο λογικός διαχωρισμός, η αρχιτεκτονική και οι ζώνες ασφαλείας του δικτύου

b) Η διαμόρφωση κάθε συσκευής πρέπει να τεκμηριώνεται λεπτομερώς. Η τεκμηρίωση αυτή πρέπει να ενημερώνεται κάθε φορά που λαμβάνει χώρα οποιαδήποτε αλλαγή.

c) Η απομακρυσμένη διαχείριση των δικτυακών συσκευών πρέπει να γίνεται μόνο με τη χρήση κρυπτογραφημένων συνδέσεων.

d) Ο έλεγχος και η καταγραφή πρέπει να ενεργοποιούνται σύμφωνα με τις πολιτικές και τις διαδικασίες ελέγχου της Εταιρείας.

e) Η πρόσβαση σε όλες τις συσκευές δικτύων της Εταιρείας πρέπει να συμμορφώνεται με τις πολιτικές "Λογική Πρόσβαση" και "Ταυτοποίηση και Αυθεντικοποίηση".

f) Οποιαδήποτε περιττή υπηρεσία πρέπει να τίθεται εκτός λειτουργίας. (π.χ. εάν ένας δρομολογητής δεν διαχειρίζεται με χρήση του SNMP, τότε το SNMP πρέπει να τεθεί εκτός λειτουργίας).

g) Οι συσκευές δικτύων πρέπει να τοποθετούνται σε εγκαταστάσεις με ελεγχόμενη πρόσβαση σύμφωνα με την "Πολιτική

Φυσικής Ασφάλειας" της Εταιρείας.

h) Το λογισμικό επιδιόρθωσης και οι αναβαθμίσεις ασφάλειας πρέπει να εφαρμόζονται έγκαιρα

i) Η Εταιρεία πρέπει να χρησιμοποιεί συστήματα Firewall και άλλες συσκευές ασφάλειας για να παρέχει φιλτράρισα και έλεγχο της κυκλοφορίας σε όλες τις εξωτερικές συνδέσεις επικοινωνίας.

1) Η Εταιρεία πρέπει να χρησιμοποιεί Firewall και Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System) σε όλες τις συνδέσεις με το Διαδίκτυο.

2) Για τις συνδέσεις με θυγατρικές εταιρείες πρέπει να χρησιμοποιούνται δρομολογητές με χαρακτηριστικά Firewall

(πχ. Packet filtering, logging).

3) Η κυκλοφορία από τα εξωτερικά συστήματα προς την Εταιρεία πρέπει να φιλτράρεται ώστε να επιτρέπεται μόνο η ελάχιστη πρόσβαση που απαιτείται για να καλύψει τις επιχειρησιακές ανάγκες της Εταιρείας.

4) Τα Firewall συστήματα πρέπει να διαμορφώνονται και να διαχειρίζονται σύμφωνα με τις καλύτερες πρακτικές που εφαρμόζονται διεθνώς στις τεχνολογίες πληροφορικής και επικοινωνιών. Ενδεικτικά, και όχι περιοριστικά, αυτές περιλαμβάνουν τα ακόλουθα:

- Τα εξ' ορισμού φίλτρα πρέπει να ορίζουν ότι οποιαδήποτε πρόσβαση στην Εταιρεία απαγορεύεται εκτός αν συγκεκριμένα επιτρέπεται.
- Κάθε Firewall και άλλη συσκευή ασφάλειας περιμέτρου πρέπει να παρακολουθείται ενεργά και να ελέγχεται περιοδικά για τυχόν απειλές στο δίκτυο της Εταιρείας.
- Τα Firewall συστήματα πρέπει να παρέχουν ειδοποιήσεις σε πραγματικό χρόνο στους διαχειριστές, σε περιπτώσεις περιστατικών ασφάλειας.
- Τα Firewall συστήματα πρέπει να χρησιμοποιούνται χωρίς διακοπή 24 ώρες το 24ωρο, 365 μέρες το χρόνο.
- Για κάθε σύστημα Firewall στις διασυνδέσεις της Εταιρείας με το Δδιαδίκτυο απαιτείται να υπάρχει εφεδρικό

  Firewall.

- Σε περίπτωση αποτυχίας συστήματος (system failure), τα Firewall πρέπει να προκαθορίζονται σε "Deny All" διάρθρωση μέχρι να επαναρυθμιστούν από ένα διαχειριστή.
- Εφόσον είναι εφικτό, οι υπηρεσίες Firewall πρέπει να τρέχουν σ' ένα αφιερωμένο σύστημα με όλες τις άλλες υπηρεσίες απενεργοποιημένες.
- Το "Source Routing" πρέπει να τεθεί εκτός λειτουργίας σ' όλα τα Firewall συστήματα και εξωτερικούς δρομολογητές.
- Τα Firewall δεν πρέπει να δέχονται την κυκλοφορία στις εξωτερικές διεπαφές τους (interfaces) που εμφανίζεται να προέρχεται από τις διευθύνσεις των εσωτερικές δικτύων.
- Πρέπει να γίνεται λήψη εφεδρικών αντιγράφων της διαμόρφωσης Firewall (λογισμικό συστήματος, δεδομένα διαμόρφωσης, αρχεία βάσεων δεδομένων, κλπ) σε καθημερινή, εβδομαδιαία και μηνιαία βάση, έτσι ώστε σε περίπτωση αποτυχίας του συστήματος τα δεδομένα και τα αρχεία διαμόρφωσης να μπορούν να ανακτηθούν. Τα εφεδρικά αντίγραφα πρέπει να προστατεύονται έτσι ώστε τα μέσα να είναι προσιτά μόνο στο κατάλληλο προσωπικό.
- Μόνο οι διαχειριστές των Firewall πρέπει να έχουν δικαιώματα για την ενημέρωση των εκτελέσιμων ή άλλου λογισμικού συστήματος..

- Οι διαχειριστές Firewall πρέπει να αξιολογούν κάθε νέα έκδοση του Firewall λογισμικού ώστε να καθορίζουν εάν απαιτείται μια αναβάθμιση. Όλες οι αναβαθμίσεις ασφάλειας (λογισμικό επιδιόρθωσης) που συστήνονται από τον κατασκευαστή του Firewall λογισμικού πρέπει να εφαρμοστούν κατά έγκαιρο τρόπο.
- Όλες οι υπηρεσίες και η κυκλοφορία που εγκρίνονται στα συστήματα Firewall πρέπει να τεκμηριώνονται. Η τεκμηρίωση πρέπει να περιέχει την επιχειρησιακή ανάγκη, το χρησιμοποιούμενο πρωτόκολλο, εάν είναι εισερχόμενη ή/και εξερχόμενη κίνηση, τις δικτυακές πόρτες, γνωστές ευπάθειες και πληροφορίες που αφορούν τον μετριασμό κινδύνου.
- Η διαμόρφωση των Συστημάτων Firewall πρέπει να αποκρύβει πληροφορίες για το δίκτυο έτσι ώστε τα στοιχεία που αφορούν το εσωτερικό του δικτύου να μην διαφημίζονται στον εξωτερικό κόσμο.

J) Τα συστήματα ή οι υπηρεσίες της Εταιρείας που πρόκειται να είναι δημόσια διαθέσιμα στο διαδίκτυο πρέπει να ακολουθούν τους ακόλουθους κανόνες:

1) Τα συστήματα αυτά πρέπει να τοποθετούνται σε μια προστατευμένη αποστρατικοποιημένη ζώνη (DMZ).

2) Δεν πρέπει να αποθηκεύονται ευαίσθητα δεδομένα στα συστήματα που βρίσκονται στην αποστρατικοποιημένη Ζώνη (DMZ). Όλα τα ευαίσθητα δεδομένα πρέπει να αποθηκεύονται εσωτερικά του Firewall.

3) Η πρόσβαση από το Διαδίκτυο σ' αυτά τα συστήματα δεν πρέπει να καταστήσει τις ευαίσθητες πληροφορίες ή τα πληροφοριακά συστήματα ευάλωτα σε παραβιάσεις.

k) Οι λεπτομέρειες του εσωτερικού δικτύου της Εταιρείας δεν πρέπει να είναι ορατές ή προσιτές εξωτερικά του Firewall.

l) Κεντρικοί υπολογιστές πληρεξουσίου (Proxy Servers):

1) Όλες οι εξερχόμενες συνδέσεις προς το Διαδίκτυο πρέπει να διεκπεραιώνονται μέσω ενός Proxy Server. Ένας Proxy Server παρέχει βελτίωση της ασφάλειας με τη συγκέντρωση των υπηρεσιών σ' ένα συγκεκριμένο Η/Υ ώστε να επιτρέψει την παρακολούθηση, την απόκρυψη της εσωτερικής δομής κλπ...

m) Οποιαδήποτε απομακρυσμένη πρόσβαση στο εσωτερικό δίκτυο της Εταιρείας μέσω του Firewall (π.χ. εφαρμογές τηλεργασίας) πρέπει να χρησιμοποιεί ισχυρή αυθεντικοποίηση και κρυπτογράφηση και να συμμορφώνεται με τις πολιτικές και τις διαδικασίες απομακρυσμένης πρόσβασης της Εταιρείας.

n) Όλος ο εξοπλισμός δικτύου οφείλει να τεκμηριώνεται σύμφωνα με τις διαδικασίες τεκμηρίωσης των πληροφοριακών Συστημάτων της Εταιρείας.

o) Οποιεσδήποτε αλλαγές στον υφιστάμενο εξοπλισμό ή την ανάπτυξη νέου εξοπλισμού στο δίκτυο πρέπει να ακολουθούν τις διαδικασίες ελέγχου αλλαγής της Εταιρείας.

p) Οι πληροφορίες σχετικά με τη διαμόρφωση του Firewall και άλλης προστασίας δικτύου θεωρούνται εμπιστευτικές και πρέπει να προστατεύονται ως ευαίσθητα δεδομένα.

q) Όλο το υλικό και λογισμικό που χρησιμοποιείται στο δίκτυο πρέπει να συμμορφώνεται με της πολιτικές και διαδικασίες ασφάλειας Συστημάτων της Εταιρείας, συμπεριλαμβανομένης και της απενεργοποίησης των μη αναγκαίων υπηρεσιών.

r) Όλα τα σχετικά με την ασφάλεια γεγονότα στον εξοπλισμό δικτύου, πρέπει να καταγράφονται και ελέγχονται σύμφωνα με τις πολιτικές και διαδικασίες "Audit Trails" της Εταιρείας.

s) Η ευθύνη για την ασφάλεια οποιουδήποτε εξοπλισμού που αναπτύσσεται από τους εξωτερικούς φορείς παροχής

υπηρεσιών, πρέπει να διευκρινίζεται στη σύβαση με το φορέα παροχής υπηρεσιών.

t) Οι υπάλληλοι πρέπει να έχουν πρόσβαση στο Διαδίκτυο μόνο μέσω των εγκεκριμένων σημείων πρόσβασης

Διαδικτύου της Εταιρείας. Οποιαδήποτε μορφή επικοινωνίας από/προς σταθμούς εργασίας έξω από το εσωτερικό

(έμπιστο) δίκτυο δεν επιτρέπεται χωρίς έγκριση. Αυτό περιλαμβάνει τα modems, τις μισθωμένες γραμμές σε άλλα δίκτυα, κ.λπ.

u) Η εταιρεία οφείλει να διατηρεί αρχείο με πλήρη ανάλυση των μέτρων προστασίας και ασφάλειας που έχουν υλοποιηθεί σε αυτά, με σκοπό την προστασία του απορρήτου των επικοινωνιών.

4.2 Ρόλοι & Υπευθυνότητες

- Ο Υπεύθυνος Πολιτικής Ασφάλειας Δικτύου φέρει την ευθύνη για:
  - Τον καθορισμό της πολιτικής και τον έλεγχο της εφαρμογής της
  - Την αποκλειστική πρόσβαση στις αποθηκευμένες δικτυακές συνόδους
  - Την διεξοδική ανάλυση των κρίσιμων περιστατικών ασφάλειας
- Οι ιδιοκτήτες των πληροφοριών φέρουν την ευθύνη για τη διασφάλιση των πόρων που τους ανήκουν σύμφωνα με τις οδηγίες που ορίζονται σ' αυτήν την πολιτική, συμπεριλαμβανομένων ενδεικτικά και όχι περιοριστικά:
  - Της εξασφάλισης των κατάλληλων εγκρίσεων και συμφωνιών για:

    i. Οποιεσδήποτε εξωτερικές συνδέσεις χρειάζονται από τα συστήματα τους

    ii. Οποιαδήποτε συστήματα ή υπηρεσίες που τους ανήκουν και τοποθετούνται εξωτερικά των Firewall Συστημάτων της Εταιρείας

    iii. Την εξωτερική πρόσβαση μέσω της περιμέτρου της Εταιρείας στα συστήματα τους που βρίσκονται στο εσωτερικό δίκτυο της Εταιρείας
  - Της εφαρμογής των κατάλληλων μέτρων προστασίας δικτύου σε οποιουσδήποτε εξωτερικά προσβάσιμους
    πόρους που τους ανήκουν
- Οι υπεύθυνοι Συστημάτων φέρουν την ευθύνη για:

  i. την παροχή βοήθειας στους ιδιοκτήτες των πληροφοριών στην εφαρμογή και διαχείριση πολιτικής δικτύου και της διαμόρφωσης Συστημάτων για τη συμμόρφωση με την παρούσα πολιτική

  ii. την παροχή βοήθειας στο Τμήμα Ασφάλειας στον έλεγχο της περιμετρικής προστασίας και της διαμόρφωσης Συστημάτων.

  iii. την άμεση αναφορά οποιασδήποτε παραβίασης της πολιτικής ή πιθανής ευπάθειας στο Τμήμα Ασφάλειας
- Οι χρήστες φέρουν την ευθύνη να προσπελαύνουν το Διαδίκτυο και άλλα εξωτερικά συστήματα μόνο μέσω των εγκεκριμένων συνδέσεων της Εταιρείας και σύμφωνα με τις διαδικασίες ασφάλειας της Εταιρείας.
- Οι προϊστάμενοι φέρουν την ευθύνη για την διασφάλιση ότι οι υπάλληλοί τους κατανοούν και συμμορφώνονται με την παρούσα πολιτική.
- Το Τμήμα Ασφάλειας φέρει την ευθύνη για:

  I. Τον έλεγχο των πληροφοριακών πόρων της Εταιρείας για τη συμμόρφωση με την παρούσα πολιτική

II. Την επισκόπηση και την έγκριση της πρόσβασης, της διασύνδεσης και των υπηρεσιών που παρέχονται

μεταξύ του δικτύου της Εταιρείας και των εξωτερικών Συστημάτων

III. Την παροχή οδηγιών στους ιδιοκτήτες των πληροφοριών και τους διαχειριστές Συστημάτων σχετικά με την ασφάλεια περιμέτρου

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

XVIII. ΠΟΛΙΤΙΚΗ ΕΛΕΓΧΟΥ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

1.0 Εισαγωγή

Ο έλεγχος εφαρμογής της Πολιτικής Ασφάλειας ανήκει σε μία «κυκλική» διαδικασία διαχείρισης της ασφάλειας η οποία ξεκινάει από τον Σχεδιασμό (PLAN), περνάει στην Λειτουργία (DO), και συνεχίζει με τον Έλεγχο (CHECK) ο οποίος έχει σαν σκοπό να εντοπίσει πιθανές ευπάθειες και να δημιουργήσει λύσεις / προτάσεις για κάθε μία από αυτές.

2.0 Σκοπός

Σκοπός αυτής της πολιτικής είναι να καθορίσει τις απαιτήσεις και το πλαίσιο διεξαγωγής ελέγχων εφαρμογής της Πολιτικής

Ασφάλειας.

3.0 Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλα τα συστήματα, δίκτυα, εφαρμογές και λοιπούς πληροφοριακούς πόρους που ανήκουν ή χρησιμοποιούνται από την Εταιρεία.

4.0 Πολιτική

4.1 Διαδικασίες & Οδηγίες

- Η εταιρεία πρέπει να προβαίνει σε έλεγχο εφαρμογής της Πολιτικής Ασφάλειας ο οποίος να καλύπτει όλο το εύρος εφαρμογής της Πολιτικής.
- Ο έλεγχος πρέπει να διεξάγεται τουλάχιστον ανά δύο έτη, και είναι δυνατόν να πραγματοποιείται από εξουσιοδοτημένους εργαζόμενους της εταιρείας.

  Αυτοί θα πρέπει να είναι κατάλληλα εκπαιδευμένοι και να λαμβάνονται υπόψη παράγοντες αντικειμενικότητας και αμεροληψίας. Ενδεικτικά αναφέρεται ότι οι ελεγκτές δεν θα πρέπει να ανήκουν στο Τμήμα ή τη Διεύθυνση της οποίας τα συστήματα ελέγχονται ή να έχουν συμμετάσχει στην ανάπτυξη κώδικα και στην εγκατάσταση ή τη λειτουργία του υπό έλεγχο συστήματος.
- Οι αρμοδιότητες των εργαζομένων της εταιρείας, οι οποίοι διενεργούν τους ελέγχους, πρέπει να είναι εκ των προτέρων καθορισμένες και να περιγράφονται αναλυτικά σε σχετικό αρχείο, το οποίο τηρείται από την εταιρεία.
- Οι διαδικασίες για τον έλεγχο πρέπει να είναι σαφώς καθορισμένες και τεκμηριωμένες.

- Οι διαδικασίες αυτές πρέπει να περιλαμβάνουν τα ακόλουθα στάδια:

1. **Προετοιμασία Ελέγχου**

   - Καθορισμός προσώπων που απαρτίζουν την ομάδα ελέγχου και καθορισμός χρονοδιαγράμματος διεξαγωγής ελέγχου.

- Καθορισμός Συστημάτων και διαδικασιών που θα ελεγχθούν.
- Συλλογή απαιτούμενων πληροφοριών και δεδομένων.
- Τα στοιχεία της παρούσας παραγράφου καταγράφονται σε σχετικό αρχείο, το οποίο διατηρείται από την εταιρεία.

2. Διεξαγωγή Ελέγχου

- Διεξαγωγή συνεντεύξεων και συζητήσεων της ομάδας ελέγχου με τους υπεύθυνους Συστημάτων, δικτύων, εφαρμογών.
- Καταγραφή αρχείου με τα σχετικά ευρήματα, προτεινόμενες βελτιώσεις ή τροποποιήσεις.
- Απαιτούμενη τεχνική έρευνα η οποία περιλαμβάνει την ανίχνευση (scanning) του ελεγχόμενου περιβάλλοντος καθώς και τη χρήση και την εξέταση των αρχείων καταγραφής, κατά περίπτωση σε συσχετισμό με άλλα αρχεία που προβλέπονται στην πολιτική ασφάλειας.
- Η απόδοση σε ένα ή περισσότερα μέλη της Ομάδας Ελέγχου δικαιωμάτων πρόσβασης σε εργαλεία λογισμικού, συστήματα (αναφέρονται ενδεικτικά τα συστήματα ανίχνευσης επισυνδέσεων) ή χώρους των εγκαταστάσεων, θα πρέπει να επιτρέπεται μόνο για το χρονικό διάστημα του αντίστοιχου ελέγχου και να γίνεται σύμφωνα με τις αντίστοιχες Πολιτικές Ασφάλειας της εταιρείας.

3. Αποτελέσματα ελέγχου

- Επεξεργασία και η ανάλυση των δεδομένων που συγκεντρώθηκαν από τα παραπάνω βήματα
- Δημιουργία αναφοράς η οποία απεικονίζει την παρούσα κατάσταση, τις πιθανές ευπάθειες που περικλείονται σε αυτήν και τέλος μια λίστα με τις προτάσεις/ λύσεις για την μείωση ή απαλοιφή τους

4.2 Ρόλοι & Υπευθυνότητες

a. Οι Ιδιοκτήτες Πληροφοριών και τα διοικητικά στελέχη της Εταιρείας φέρουν την ευθύνη για:

1) Τη δέσμευση στην διεξαγωγή ελέγχων εφαρμογής Πολιτικής Ασφάλειας των Πληροφοριακών Συστημάτων.

2) Να λαμβάνουν υπ' όψιν τα αποτελέσματα των ελέγχων στη λήψη των αποφάσεων για τη χρήση πληροφοριακών πόρων.

3) Την εφαρμογή των κατάλληλων μέτρων προστασίας βάσει των αποτελεσμάτων ελέγχου εφαρμογής της Πολιτικής

Ασφάλειας

b. Οι Υπεύθυνοι Συστημάτων, Δικτύων και Εφαρμογών φέρουν την ευθύνη για:

1) Την παροχή βοήθειας με σκοπό την διεξαγωγή ελέγχου εφαρμογής της Πολιτικής Ασφάλειας.

2) Την εφαρμογή των κατάλληλων μέτρων προστασίας βάσει των αποτελεσμάτων ελέγχου εφαρμογής της Πολιτικής

Ασφάλειας.

c. Το Τμήμα Ασφάλειας φέρει την ευθύνη για:

1) Την ανάπτυξη των διαδικασιών ελέγχου εφαρμογής της Πολιτικής Ασφάλειας.

2) Την κοινοποίηση των ευπαθειών στους Ιδιοκτήτες Πληροφοριών και τους Υπεύθυνους Συστημάτων.

3) Τη διεξαγωγή ελέγχου για να διασφαλιστεί ότι οι ευπάθειες έχουν μμετριαστεί.

4) Την παροχή συμβουλών στους Ιδιοκτήτες Πληροφοριών και τους Υπεύθυνους Συστημάτων με τις πιθανές στρατηγικές μμετριασμού των ευπαθειών.

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	Ημερομηνία	Αλλαγές
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

ΧΙΧ. ΠΟΛΙΤΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

1.0 Εισαγωγή

Τα κακόβουλα λογισμικά υπολογιστών είναι προγράμματα που αναπαράγονται και συχνά προσπαθούν να προκαλέσουν ζημιά στους υπολογιστές που μολύνουν. Τα λογισμικά αυτά μπορούν να καταστρέψουν δεδομένα, να καταστήσουν τους υπολογιστές ακατάλληλους προς χρήση, να χρησιμοποιήσουν τον υπολογιστή για να επιτεθούν σε άλλους υπολογιστές ή να εκτελέσουν ποικίλες άλλες κακόβουλες δραστηριότητες.
Η χρήση προγραμμάτων ανίχνευσης κακόβουλου λογισμικού είναι ουσιαστική για την προστασία των πόρων της Εταιρείας από κινδύνους που προέρχονται από ιούς υπολογιστών και άλλα κακόβουλα προγράμματα. Τα προγράμματα ανίχνευσης/προστασίας κακόβουλου λογισμικού ανιχνεύουν για στοιχεία ύπαρξης τέτοιου λογισμικού στους υπολογιστές της Εταιρείας και προσπαθούν να το αφαιρέσουν προτού να διαδοθεί ή να προκαλέσει περαιτέρω ζημία.
Ωστόσο, τα προγράμματα ανίχνευσης κακόβουλου λογισμικού χρειάζονται κάποιο χρονικό διάστημα προκειμένου να ενημερωθούν για κάθε "νέο" λογισμικό που δημιουργείται, κατά τη διάρκεια του οποίου το "νέο" λογισμικό μπορεί να προκαλέσει σοβαρή ζημιά. Επομένως, είναι σημαντικό οι χρήστες και οι διαχειριστές Συστημάτων να γνωρίζουν τους κινδύνους που προέρχονται από τα κακόβουλα λογισμικά και να λαμβάνουν μέτρα για να ελαχιστοποιήσουν την έκθεση σ' αυτά.

2.0 Σκοπός

Σκοπός της πολιτικής είναι η εφαρμογή πρότυπου λογισμικού και διαδικασιών για την ελαχιστοποίηση του αντίκτυπου των κακόβουλων λογισμικών στους πόρους Πληροφοριακών Συστημάτων της Εταιρείας.

3.0 Πεδίο εφαρμογής

Η παρούσα πολιτική ισχύει για όλους τους κεντρικούς υπολογιστές και τους σταθμούς εργασίας της Εταιρείας, καθώς επίσης και για οποιοδήποτε υπολογιστή χρησιμοποιείται για απομακρυσμένη πρόσβαση στο δίκτυο της Εταιρείας.

4.0 Πολιτική

4.1 Διαδικασίες & Οδηγίες

- Οι κεντρικοί υπολογιστές και σταθμοί εργασίας πρέπει να τρέχουν το πρότυπο πρόγραμμα ανίχνευσης κακόβουλου λογισμικού που υποστηρίζεται από την Εταιρεία.
- Η εταιρεία σε συμφωνία με τις αρχές Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών οφείλει να πραγματοποιεί έλεγχο της ακεραιότητας του λογισμικού των ΟΠΣ με σκοπό τη διαπίστωση της μη ύπαρξης λογισμικού πέραν αυτού που έχει επισήμως προμηθευτεί η εταιρεία.
- Η Εταιρεία χρησιμοποιεί το πρόγραμμα ανίχνευσης κακόβουλου λογισμικού στην πύλη ηλεκτρονικού ταχυδρομείου για την ανίχνευση των μηνυμάτων και των συνημμένων.
- Οι χρήστες δεν μπορούν να θέσουν εκτός λειτουργίας το πρόγραμμα ανίχνευσης κακόβουλου λογισμικού για οποιοδήποτε λόγο.
- Το πρόγραμμα ανίχνευσης κακόβουλου λογισμικού πρέπει να ενημερώνεται αυτόματα μόλις οι νέες υπογραφές ιών υπολογιστών παρέχονται από τον κατασκευαστή.

- Οποιοσδήποτε υπολογιστής χρησιμοποιείται για απομακρυσμένη πρόσβαση στο δίκτυο της Εταιρείας (όπως ένας φορητός υπολογιστής που χρησιμοποιείται για τηλεργασία) πρέπει να έχει εγκεκριμένο πρόγραμμα ανίχνευσης κακόβουλου λογισμικού που φορτώνεται και ενημερώνεται σε κανονική βάση.
- Οποιαδήποτε μολυσμένα αρχεία που δεν μπορούν να επισκευαστούν πρέπει να απομονώνονται (quarantined) ή να διαγράφονται.
- Οι μολυσμένοι υπολογιστές που δεν μπορούν να καθαριστούν από το πρόγραμμα ανίχνευσης κακόβουλου λογισμικού πρέπει να αφαιρούνται από το δίκτυο έως ότου επιβεβαιωθεί ότι είναι καθαροί από οποιοδήποτε κακόβουλο λογισμικό.
- Οι υπάλληλοι πρέπει να ενημερώνονται για τεχνικές αποφυγής κακόβουλου λογισμικού, συμπεριλαμβανομένου των
ακόλουθων οδηγιών:

  Μην ανοίγετε αρχεία συνημμένα σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που προέρχεται από μια άγνωστη ή μη έμπιστη πηγή. Διαγράψτε αμέσως τα συνημμένα αρχεία και αδειάστε το κάδο ανακύκλωσης.

  Διαγράψτε τα αυτόκλητα μηνύματα ηλεκτρονικού ταχυδρομείου (Spam), τα "chain letters" ή άλλα "junk mail" χωρίς να τα προωθήσετε.

  Σε μηνύματα στα οποία ο αποστολέας είναι γνωστός ή φαίνεται έμπιστος εξετάστε αν το περιεχόμενο του μηνύματος ταιριάζει στον αποστολέα (αγγλικό κείμενο από Έλληνα αποστολέα,...).

  Εξετάστε αν στο μήνυμα που λάβατε ταιριάζουν τα συνημμένα.

  - Προσοχή όταν λαμβάνετε περισσότερα μηνύματα με το ίδιο θέμα (subject).
  - Μην προωθείτε μηνύματα με περιεχόμενο που προειδοποιεί για ιούς ή μηνύματα που το περιεχόμενο τους σας προτρέπει να τα προωθήσετε.

  - Μην κατεβάζετε (download) αρχεία από άγνωστες ή ύποπτες πηγές στο Διαδίκτυο.

- Όλα τα φορητά μέσα αποθήκευσης (π.χ. USB sticks, εξωτερικοί δίσκοι κλπ) πρέπει να ανιχνεύονται με το πρόγραμμα ανίχνευσης κακόβουλου λογισμικού πριν από τη χρήση τους σ' έναν υπολογιστή της Εταιρείας.
- Εάν οι εργαστηριακές δοκιμές έρχονται σε σύγκρουση με το πρόγραμμα ανίχνευσης κακόβουλου λογισμικού, τρέξτε το πρόγραμμα ανίχνευσης κακόβουλου λογισμικού για να εξασφαλιστεί ότι ο υπολογιστής είναι καθαρός, θέστε εκτός λειτουργίας το πρόγραμμα και στη συνέχεια εκτελέστε την εργαστηριακή δοκιμή. Μετά από την εργαστηριακή δοκιμή ενεργοποιήστε το πρόγραμμα ανίχνευσης κακόβουλου λογισμικού.
- Η Εταιρεία οφείλει να διατηρεί αρχείο στο οποίο θα τεκμηριώνονται οι λεπτομέρειες εφαρμογής των απαιτήσεων που καταγράφονται στην συγκεκριμένη Πολιτική.

4.2 Ρόλοι και Υπευθυνότητες

- Το Τμήμα Συστημάτων και Υπηρεσιών φέρει την ευθύνη για την εγκατάσταση των προγραμμάτων ανίχνευσης κακόβουλου λογισμικού στους σταθμούς εργασίας και τους κεντρικούς υπολογιστές.
- Το Τμήμα Τεχνικής Υποστήριξης σε συνεργασία με το Τμήμα Συστημάτων & Υπηρεσιών φέρει την ευθύνη για τον εντοπισμό και την αφαίρεση κακόβουλου λογισμικού, την απομόνωση των προσβεβλημένων Συστημάτων και την παροχή υποστήριξης στους χρήστες ώστε να κατανοήσουν τις διαδικασίες και τις οδηγίες προστασίας από κακόβουλο λογισμικό.
- Το Τμήμα Ασφάλειας είναι αρμόδιο για τον έλεγχο των Πληροφοριακών Συστημάτων ώστε να διασφαλίσει ότι οι χρήστες συμμορφώνονται με τις πολιτικές και τις διαδικασίες διαχείρισης των προγραμμάτων ανίχνευσης κακόβουλου λογισμικού της Εταιρείας.

- Το Τμήμα Ασφάλειας σε συνεργασία με το Τμήμα Συστημάτων και Υπηρεσιών φέρουν την ευθύνη για τη διαχείριση των μέτρων προστασίας από ιούς και την επανεξέταση της πολιτικής προστασίας από κακόβουλο λογισμικό.

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	**Ημερομηνία**	**Αλλαγές**
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

XX. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ ΣΥΣΤΗΜΑΤΩΝ

1.0 Εισαγωγή

Οι κωδικοί ασφάλειας πρόσβασης (passwords) είναι βασικό στοιχεία ασφάλειας τόσο των προσωπικών όσο κ των εταιρικών δεδομένων.
Λάθος επιλογή κωδικού μπορεί να προκαλέσει απώλεια είτε μη εγκεκριμένη αλλαγή, των εταιρικών δεδομένων.

2.0 Σκοπός

Σκοπός της πολιτικής είναι η εξασφάλιση ασφαλέστερης επιλογής κωδικού πρόσβασης (password)

3.0 Πεδίο εφαρμογής

Η παρούσα πολιτική ισχύει για μόνιμους είτε outsourced υπαλλήλους, καθώς και εξωτερικούς συνεργάτες, είτε με φυσική παρουσία στο εταιρικό δίκτυο είτε απομακρυσμένα.
Αφορά κάθε είδος κωδικού συμπεριλαμβανομένων των email & Domain accounts, web,, Database, ERP, network & other similar devices.

4.0 Πολιτική

4.1 Κανόνες βελτιωμένης Ασφάλειας
4.1.1 Κανόνες για βελτιωμένα passwords:

- Πρέπει να περιέχει τουλάχιστον 9 χαρακτήρες (μέγιστο προτεινόμενο 14)
- Πρέπει να περιέχει κεφαλαία κ πεζά γράμματα
- Πρέπει να περιέχει τουλάχιστον 1 αριθμό (π.χ., 0-9)
- Να αποτελείτε από συνδυασμό 2 ή περισσότερων λέξεων
- Πρέπει να περιέχει τουλάχιστον 1 ειδικό χαρακτήρα (π.χ., ,!$%^&*()_+|~-=\`{}[]:";'<>?,/)

4.1.2 Λανθασμένα passwords:

- Με μέγεθος μικρότερο από 8 χαρακτήρες
- Λέξεις από λεξικό (ελληνικό ή άλλο)
- Εταιρικοί κωδικοί ίδιοι με κωδικούς σε unsecure web sites
- Επαναλαμβανόμενοι κωδικοί (προτείνονται πάνω από 10 μη επαναλαμβανόμενοι κωδικοί)
- Περιέχουν μέρος ή το σύνολο του username string
- Περιέχουν προσωπικά στοιχεία (γενέθλιά, διευθύνσεις, τηλέφωνα, ή ονόματα μελών της οικογένειας/φίλων)
- Περιέχουν στοιχεία σχετικά με το εταιρικό περιβάλλον (όνομα εταιρίας, εντολές συστημάτων ή ονόματα κατασκευαστών)
- Περιέχουν γραμματοσειρές του τύπου: aaabbb, qwerty, 123456, κλπ
- Κοινές λέξεις με αριθμούς που προηγούνται είτε έπονται, όπως :secret1, 2test κλπ

Οι κωδικοί πρόσβασης δεν θα πρέπει να γράφονται αλλά να απομνημονεύονται εύκολα.

Θα μπορούσαν να είναι τα αρχικά από μία φράση όπως: APTRFALLWEB ("A Password To Remember For Allweb"

4.2 Κανόνες προστασίας κωδικών πρόσβασης

Οι κωδικοί πρέπει:

- Να αλλάζουν τουλάχιστον κάθε 3-4 μήνες
- Να μην αποκαλύπτονται με κανέναν τρόπο (τηλεφωνικά, μέσω emails, είτε σε κάποια φόρμα/ερωτηματολόγιο
- Να μην αποθηκεύονται σε αρχεία ή άλλου είδους κείμενα
- Να μην αποθηκεύονται σε browsers με την επιλογή «Remember Password"

Ειδικότερα και σχετικά με την ανάπτυξη εφαρμογών:

- Να υποστηρίζεται το authentication χρηστών κ όχι μόνο ομάδας (group)
- Να μην αποθηκεύονται σε clear test αλλά encrypted
- Να μην μεταφέρονται μέσα από το δίκτυο σε clear text
- Να υποστηρίζεται ο ρόλος του "Role Manager" ο οποίος θα μπορεί να επεμβαίνει σε άλλους χρήστες χωρίς την γνώση του password
- Να υπάρχει ενημέρωση κ συνεργασία των developers με την ομάδα ασφάλειας νωρίς στον κύκλο ανάπτυξης εφαρμογών, για την καλύτερη υλοποίηση της πολιτικής.

4.3 Allweb Solutions S.A. password management

Οι κωδικοί αποθηκεύονται σε encrypted database, με διαβαθμισμένη πρόσβαση ανά τεχνικό και ανά τμήμα, σε περιορισμένη ομάδα χρηστών.

4.4 Επιβολή Πολιτικής

Ο υπεύθυνος ασφάλειας μπορεί να διενεργεί ελέγχους μέσα από διάφορες διαδικασίες όπως με την χρήση audit εργαλείων, αυτοψιών, κλπ

Κάθε εξαίρεση στους παραπάνω κανόνες θα πρέπει να προ-εγκρίνεται από τον υπεύθυνο ασφαλείας.

Περιπτώσεις απώλειας κωδικού είτε διαρροή του με οποιονδήποτε τρόπο θα πρέπει να αναφέρεται άμεσα και να αντικαθίστανται με άλλον.

5.0 Αναθεώρηση και Αξιολόγηση

- Το Τμήμα Ασφάλειας φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).
- Η εξασφάλιση της επικαιρότητας της Πολιτικής Ασφάλειας, καθώς και η διασφάλιση ότι το προσωπικό γνωρίζει το εκάστοτε ισχύον κείμενο, αποτελεί ευθύνη του Τμήματος Ασφάλειας.

6.0 Ιστορικό Αναθεώρησης

Έκδοση	Ημερομηνία	Αλλαγές
0.1	15/03/2016	1η επίσημη έκδοση
1.0	15/12/2016	Αναθεώρηση
2.0	15/10/2020	Αναθεώρηση

XXI. ΠΟΛΙΤΙΚΗ ΑΝΤΑΛΛΑΓΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η ανταλλαγή ευαίσθητων δεδομένων μέσω emails είτε εντός είτε εκτός της εταιρείας γενικά πρέπει να αποφεύγεται.
Σαν ευαίσθητα δεδομένα συμπεριλαμβάνονται, τα δεδομένα πελατών της εταιρείας, οικονομικά στοιχεία, στοιχεία εμπορικής στρατηγικής ή στοιχεία marketing.

Εάν για οποιοδήποτε λόγο κριθεί απαραίτητη η αποστολή μέσω ηλεκτρονικού ταχυδρομείου ευαίσθητων δεδομένων, τότε θα πρέπει να γίνεται κρυπτογραφημένα σύμφωνα με τη διαδικασία ανταλλαγής πληροφοριών.

Η Εταιρεία προκειμένου να υλοποιεί ολοκληρωμένες υπηρεσίες με εταιρικούς πελάτες απαιτεί να υπάρχει μία ενιαία γραμμή πλεύσης και σαφείς οδηγίες για την πραγματοποίηση των συνδέσεων που να εξασφαλίζει μια ορισμένη ασφάλεια Η ανάλυση θα πρέπει να γίνει στους παρακάτω τομείς:

1. Εντοπισμός τρωτών σημείων στα συστήματα διοίκησης και λογιστικής όπου οι πληροφορίες κατανέμονται ανάμεσα σε διαφορετικές ομάδες της εταιρείας.
2. Εντοπισμός τρωτών σημείων (vulnerabilities) στα επικοινωνιακά συστήματα, όπως τα αποθηκευμένα τηλεφωνικά μηνύματα, η εμπιστευτικότητα των κλήσεων, τα ανοικτά email.
3. Εφαρμογή πολιτικής και ελέγχων διαχείρισης ανταλλαγής πληροφοριών
4. Περιορισμός πρόσβασης σε ευαίσθητα προσωπικά δεδομένα που σχετίζονται με το προσωπικό
5. Κατηγορίες προσωπικού που έχει πρόσβαση στο σύστημα και αιτιολόγηση της χρήσης του συστήματος
6. Διατήρηση αντιγράφων ασφάλειας του συστήματος
7. Διαδικασίες συνέχισης εργασιών.

XXII. ΜΗΤΡΩΟ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ IT

Τα περιουσιακά στοιχεία πληροφορικής όπως για παράδειγμα

- Τα εργαλεία λογισμικού για την ανάπτυξη εφαρμογών λογισμικού
- Τα εργαλεία λογισμικού για την διαχείριση έργων
- Τα συστήματα

θα βρίσκονται καταγεγραμμένα σε ένα η περισσότερα μητρώα.
Κάθε μητρώο θα έχει έναν υπεύθυνο ιδιοκτήτη ο οποίος θα επιτελεί τον ρόλο του «Υπεύθυνου Μητρώου».

XXIII. ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ (RISK MANAGEMENT)

Η προστασία των περιουσιακών στοιχείων που θα βρίσκονται καταγεγραμμένα στα μητρώα θα βασίζεται σε αποτίμηση των αδυναμιών τους και των κινδύνων που τα απειλούν.

Η αποτίμηση των κινδύνων λαμβάνει υπόψη :

- Την συμβολή κάθε στοιχείου στην αποστολή της εταιρείας
- Τις αδυναμίες
- Τους κινδύνους
- Τις επιπτώσεις από ενδεχόμενη προσβολή
- Μοναδικά σημεία αστοχίας
- Μέθοδο ποσοτικοποίησης και αποτίμησης των κινδύνων
- Τρόπους μείωσης των επιπτώσεων μέσω εφαρμογής μέτρων προστασίας.

Η διαχείριση κινδύνων ακολουθεί συγκεκριμένη μεθοδολογία και έχει ως αποτέλεσμα ένα «Σχέδιο Αντιμετώπισης Κινδύνων», το οποίο αναθεωρείται σε τακτά χρονικά διαστήματα.

XXIV. ΠΟΛΙΤΙΚΗ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ ΚΑΙ ΑΠΟΘΗΚΕΥΤΙΚΩΝ ΜΕΣΩΝ

Οσοι χρησιμοποιούν φορητούς υπολογιστές εκτός εταιρείας φροντίζουν ώστε :

- Να επιτηρούν συνέχεια τον υπολογιστή τους
- Κρυπτογραφούν είτε να προστατεύουν με ισχυρό password τις διαβαθμισμένες πληροφορίες.

Η αποθήκευση διαβαθμισμένων πληροφοριών σε κινητά μέσα (flash drives, φορητοί δίσκοι, μαγνητικά και οπτικά) αποθηκευσης πρέπει να αποφεύγεται.

Σε περιπτώσεις που απαιτείται μεταφορά πληροφοριών μέσω κινητων μέσων πρέπει να δίνεται προσοχή ώστε να τηρούνται οι απαιτήσεις ασφάλειας.

XXV. ΠΟΛΙΤΙΚΗ ΑΔΕΙΟΥ ΓΡΑΦΕΙΟΥ (CLEAR DESK)

Για τα γραφεία των μελών των ομάδων που εργάζονται στην σύνταξη προσφορών καθώς και την υλοποίηση διαβαθμισμένων έργων ακολουθείται η πολιτική άδειου γραφείου (Clear Desk).

XXVI. ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΡΥΘΜΙΣΕΩΝ ΛΟΓΙΣΜΙΚΟΥ

Για την διαχείριση των ρυθμίσεων και των τροποποιήσεων λογισμικού να ακολουθείται το υπόδειγμα "Software Configuration Management Plan (SCMP)"

Αρμόδιος για την συμπλήρωση του υποδείγματος και την προσαρμογή του στο κάθε έργο είναι ο Υπεύθυνος Εργου.

XXVII. ΠΟΛΙΤΙΚΗ ΕΠΙΧΕΙΡΗΜΑΤΙΚΗΣ ΣΥΝΕΧΕΙΑΣ (BCP)

Ο σκοπός ενός σχεδίου επιχειρηματικής συνέχειας είναι η επαναλειτουργία των κρίσιμων επιχειρησιακών διεργασιών μετά από μία απρογραμμάτιστη και απροσδόκητη διακοπή.

Η ανάπτυξη ενός σχεδίου επιχειρηματικής συνέχειας θα πρέπει να λαμβάνει υπόψη τα ακόλουθα.

1. Καθορισμό των λειτουργικών απαιτήσεων κάθε κρίσιμης διεργασίας, των απαιτούμενων ελάχιστων πόρων για την επαναλειτουργία της, της διαθεσιμότητας τηλεπικοινωνιών και κρίσιμων δεδομένων.
2. Μία αποτίμηση και ιεράρχηση των κινδύνων.
3. Την επιλογή ενός οικονομικά βιώσιμου σεναρίου, την υλοποίηση και την συντήρησή του.
4. Την ανάπτυξη και συντήρηση ενός προγράμματος ενημέρωσης και επιμόρφωσης των αποδεκτών του σχεδίου καθώς και των μελών των ομάδων που θα το υποστηρίξουν.

Οι επιχειρηματικές διεργασίας που θα ενταχθούν στο σχέδιο πρέπει να είναι εγκεκριμένες από την διοίκηση.

Ο αποδεκτός μέγιστος χρόνος αποκατάστασης της λειτουργίας μίας κρίσιμης διεργασίας μετά από διακοπή πρέπει να είναι εγκεκριμένος από την διοίκηση.