ΔΙΑΧΕΙΡΙΣΤΗΣ ΕΛΛΗΝΙΚΟΥ ΔΙΚΤΥΟΥ ΔΙΑΝΟΜΗΣ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ Α.Ε.

ΔΙΑΚΗΡΥΞΗ ΔΗΜΟΠΡΑΣΙΑΣ ΜΕ ΑΡΙΘΜΟ ΔΔ-207

ΕΡΓΟ: «Πιλοτικό Σύστημα Τηλεμέτρησης και Διαχείρισης της Ζήτησης Παροχών Ηλεκτρικής Ενέργειας Οικιακών και Μικρών Εμπορικών Καταναλωτών και Εφαρμογής Έξυπνων Δικτύων»

ΕΛΑΧΙΣΤΕΣ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΟ ΕΡΓΟ

ΠΕΡΙΕΧΟΜΕΝΑ

1 Γενικά

Όλα τα συστήματα και οι λειτουργίες του έργου πρέπει να είναι προστατευμένα από μη εξουσιοδοτημένη πρόσβαση, εκούσια ή ακούσια, να παρακολουθούνται συνεχώς και να ενημερώνονται ώστε να διασφαλίζεται ότι οι όποιες απειλές θα εντοπίζονται και θα εξουδετερώνονται εγκαίρως και απαραίτητα πριν προκαλέσουν οποιαδήποτε επίπτωση στο σύστημα, στην εταιρεία ή τον καταναλωτή.

Καθώς ο αυτοματοποιημένος έλεγχος του ενεργειακού εξοπλισμού αναπτύσσεται με τη σταδιακή εισαγωγή τεχνολογιών όπως «έξυπνα δίκτυα», η ασφάλεια και ο έλεγχος της πρόσβασης στις υποδομές, τόσο εντός όσο και εκτός της εταιρείας έχει καταστεί ιδιαίτερα κρίσιμος.

Η φυσική και λογική ασφάλεια πρέπει να εφαρμόζεται σε όλα τα επίπεδα, προκειμένου να διασφαλίζεται η ασφαλής και αποτελεσματική λειτουργία των υποσυστημάτων παρακολούθησης και ελέγχου. Η φυσική ασφάλεια - έλεγχος της πρόσβασης στο χώρο ελέγχου, για παράδειγμα, σε συνδυασμό με τη λογική ασφάλεια – με τη χρήση πληροφοριακών συστημάτων για τον περιορισμό της πρόσβασης στις λειτουργίες παρακολούθησης και ελέγχου - παρέχουν ένα αρχικό πλαίσιο στο οποίο θα καθοριστεί και θα λειτουργήσει μια υποδομή ασφαλείας που θα διασφαλίζει την επίτευξη των επιχειρησιακών στόχων με τον ελάχιστο κίνδυνο.

Τα συστήματα των εταιρειών ηλεκτρικής ενέργειας του μέλλοντος θα είναι μία συλλογή από υποσυστήματα - καθώς θα προστίθενται νέες δυνατότητες υποδομών, τα υφιστάμενα συστήματα θα πρέπει να λειτουργούν συγχρόνως με τα νέα, κατά τρόπο που δεν θα αυξάνουν τα τρωτά σημεία στις διασυνδέσεις ή δεν θα εισάγουν κινδύνους ασφαλείας στη συνεργασία των εφαρμογών/ υποσυστημάτων.

Η διαχείριση των κινδύνων ασφαλείας απαιτεί όλες οι επιχειρησιακές διαδικασίες να έχουν σαφώς καθορισθεί και τεκμηριωθεί. Στην περίπτωση των συστημάτων AMI/MDM, όλες οι διαδικασίες που περιβάλλουν τη συλλογή δεδομένων, είτε πρόκειται για εγκαταστάσεις είτε για δεδομένα που λαμβάνονται από τον καταναλωτή, θα πρέπει να έχουν καταγραφεί και αντιμετωπιστεί πριν την εγκατάσταση του συστήματος AMI/MDM.

Καθώς τα συστήματα AMI/MDM αναπτύσσονται και λειτουργούν, θα πρέπει αντίστοιχα να εντοπίζονται τα τρωτά σημεία και να αντιμετωπίζονται διαρκώς, με σαφή τεκμηρίωση. Για το σκοπό αυτό θα πρέπει να αναπτυχθούν και εφαρμοσθούν ολοκληρωμένα σχέδια ασφαλείας, ώστε οι απειλές να ελέγχονται και τα αποτελέσματα από την εφαρμογή των στρατηγικών αντιστάθμισης κινδύνων να είναι τα αναμενόμενα.

2 Απαιτήσεις Φυσικής Ασφαλείας

1. Ο Ανάδοχος θα τεκμηριώσει τις διαδικασίες σχετικά με τη συλλογή και διαχείριση των δεδομένων των πελατών που αφορούν τη *φυσική* ασφάλεια και θα αναλύσεις τους κινδύνους και τα ευάλωτα σημεία. Βάσει της ανάλυσης αυτής θα καθορίσει τις αλλαγές στις διαδικασίες για την υλοποίηση του

συστήματος AMI/MDM και θα εντοπίσει τα σημεία στα οποία οι κίνδυνοι μειώνονται, διατηρούνται ή αυξάνονται.

2. Ο Ανάδοχος θα τεκμηριώσει περιπτώσεις που σχετίζονται με τη φυσική ασφάλεια σε όλες τις επιτηρούμενες και μη επιτηρούμενες εγκαταστάσεις που σχετίζονται με το σύστημα AMI/MDM. Αυτές θα περιλαμβάνουν τα κέντρα ελέγχου, εγκαταστάσεις επικοινωνιών, χώρους αποθήκευσης δεδομένων, διατήρησης αντιγράφων ασφαλείας, κλπ.
3. Ο Ανάδοχος θα καθιερώσει και θα λειτουργήσει μία φυσική περίμετρο ασφαλείας σε όλες τις επιτηρούμενες και μη επιτηρούμενες εγκαταστάσεις που σχετίζονται με το σύστημα AMI/MDM. Αυτές θα περιλαμβάνουν τα κέντρα ελέγχου, εγκαταστάσεις επικοινωνιών, χώρους αποθήκευσης δεδομένων, διατήρησης αντιγράφων ασφαλείας, κλπ.
4. Ο Ανάδοχος θα καθορίσει και θα διασφαλίσει ότι το σύνολο του προσωπικού με φυσική πρόσβαση σε κρίσιμες εγκαταστάσεις έχει εξουσιοδοτηθεί για την πρόσβαση μόνο στο επίπεδο που απαιτείται για την εκτέλεση των καθηκόντων τους.
5. Ο Ανάδοχος θα προμηθεύσει, θα εγκαταστήσει τον απαραίτητο εξοπλισμό, θα καθορίσει και θα λειτουργήσει μία διαδικασία που περιγράφει την παρακολούθηση της ατομικής φυσικής πρόσβασης, από τη στιγμή της εισόδου μέχρι την έξοδο, που θα περιλαμβάνει ενδεικτικά και όχι περιοριστικά τα παρακάτω:
   - Παρακολούθηση με video των κέντρων ελέγχου, εγκαταστάσεων επικοινωνιών, χώρων αποθήκευσης δεδομένων, διατήρησης αντιγράφων ασφαλείας και κύριας πρόσβασης.
   - Καταγραφή με σύστημα πρόσβασης όλων των ατόμων που εισέρχονται και εξέρχονται από κρίσιμες υποδομές, συμπεριλαμβανομένων των κέντρων ελέγχου, εγκαταστάσεων επικοινωνιών, χώρων αποθήκευσης δεδομένων, διατήρησης αντιγράφων ασφαλείας, και κύριων διαδρόμων που χρησιμοποιούνται από το προσωπικό.
6. Ο Ανάδοχος θα αναπτύξει και θα υλοποιήσει ένα σχέδιο αντιμετώπισης για κάθε κρίσιμη υποδομή. Ο κύριος σκοπός του σχεδίου αντιμετώπισης είναι να διακρίνει συνήθεις ηλεκτρομηχανολογικές βλάβες από κακόβουλες ενέργειες. Για τα συμβάντα που οφείλονται σε κοινές ηλεκτρομηχανολογικές βλάβες θα καθιερωθεί μία διαδικασία για την ενημέρωση του ΔΕΔΔΗΕ σχετικά με την ανάγκη εκτέλεσης διορθωτικών ενεργειών. Για τα συμβάντα που προσδιορίζεται ότι οφείλονται σε κακόβουλες ενέργειες, θα καθιερωθεί μια διαδικασία ενημέρωσης του προσωπικού ασφαλείας και του ΔΕΔΔΗΕ, καθώς και μια διαδικασία για την απαγόρευση της πρόσβασης στην επηρεαζόμενη περιοχή.
7. Ο Ανάδοχος θα διασφαλίσει ότι το προσωπικό του, στο οποίο έχουν εκχωρηθεί δικαιώματα πρόσβασης σε κρίσιμες περιοχές, είναι το κατάλληλο να έχει πρόσβαση σε αυτές τις περιοχές χωρίς συνοδεία.
8. Ο Ανάδοχος θα διασφαλίσει ότι το σύνολο του προσωπικού του και των υπεργολάβων του είναι ενημερωμένο για τις πρακτικές ασφαλείας του ΔΕΔΔΗΕ και τις ακολουθεί πλήρως. Το προσωπικό του αναδόχου θα

υπογράψει δηλώσεις εμπιστευτικότητας πληροφοριών καθώς και αποδοχής και δέσμευσης για την τήρηση των μέτρων ασφαλείας του ΔΕΔΔΗΕ.

9. Ο Ανάδοχος θα διασφαλίσει ότι η φυσική και λογική πρόσβαση σε όλα τα συστήματα επικυρώνεται με τη χρήση κατάλληλου συστήματος (π.χ. key-card). Ο Ανάδοχος θα διασφαλίσει ότι η key-card πρέπει να παραμείνει τοποθετημένη σε συγκεκριμένο σταθμό εργασίας ώστε να διατηρηθεί η κατάσταση σύνδεσης με το σύστημα, π.χ. εφόσον έχει γίνει σύνδεση με το σύστημα (log-on), αφαίρεση της κάρτας οδηγεί σε αυτόματη αποσύνδεση (log-out).

3 Απαιτήσεις Λογικής Ασφαλείας

10. Ο Ανάδοχος θα τεκμηριώσει περιπτώσεις χρήσης σχετικά με τη συλλογή και διαχείριση των δεδομένων των πελατών που αφορούν τις πρακτικές *λογικής* ασφάλειας και θα παρουσιάσει τους κινδύνους και τα ευάλωτα σημεία. Ο Ανάδοχος θα καθορίσει τις αλλαγές σε αυτές τις περιπτώσεις χρήσης με την υλοποίηση του συστήματος AMI/MDM και θα εντοπίσει τα σημεία στα οποία οι κίνδυνοι μειώνονται, διατηρούνται ή αυξάνονται ως αποτέλεσμα της υλοποίησης του νέου AMI/MDM.
11. Ο Ανάδοχος θα αναπτύξει, τεκμηριώσει και λειτουργήσει μία διαδικασία για τον έλεγχο της ταυτοποίησης των χρηστών σε όλα τα επίπεδα στο σύστημα AMI/MDM. Ο Ανάδοχος θα διασφαλίσει ότι η διαδικασία χρησιμοποιεί μεθόδους ασφαλούς ελέγχου ταυτοποίησης για την ανάκληση ή εκχώρηση των δικαιωμάτων χρήστη, όπως απαιτείται.
12. Ο Ανάδοχος θα διασφαλίσει και επιδείξει ότι οι διαδικασίες ελέγχου ταυτοποίησης υποστηρίζουν λειτουργίες εκτάκτου ανάγκης και ότι οι διαδικασίες αυτές δεν αποτελούν εμπόδιο στη λειτουργία υπό τέτοιες συνθήκες.
13. Ο Ανάδοχος θα διασφαλίσει ότι όλοι κωδικοί χρήσης παράγονται με μοναδικό τρόπο από την αρμόδια λειτουργία του συστήματος ή ότι το σύστημα εξαναγκάζει το χρήστη να αλλάξει τον κωδικό χρήσης με την είσοδο σε αυτό.
14. Ο Ανάδοχος θα διασφαλίσει ότι όλοι οι λογαριασμοί χρήστη έχουν "ισχυρούς" κωδικούς και ότι ο χρήστης εξαναγκάζεται να αναπτύξει τέτοιους κωδικούς αν δεν τους εισάγει εξαρχής.
15. Ο Ανάδοχος θα διασφαλίσει ότι όλοι οι ρόλοι που επιτρέπουν πρόσβαση στο σύστημα (root-access) χρησιμοποιούν κλειδί ασφαλείας που παράγεται εσωτερικά και ότι η πρόσβαση αυτή δεν επιτρέπεται σε λογαριασμού όπου έχουν ενεργοποιηθεί κωδικοί από τον χρήστη.
16. Ο Ανάδοχος θα διασφαλίσει ότι όλοι οι λογαριασμοί χρήστη ακολουθούν μία ιεραρχία ρόλων, ώστε τα δικαιώματα να παρέχονται σύμφωνα με το ρόλο του χρήστη.

17. Ο Ανάδοχος θα διασφαλίσει ότι όταν ένας χρήστης απομακρύνεται από το κεντρικό σύστημα ή δεν σχετίζεται κατά κάποιον τρόπο με το έργο, θα τερματίζεται η πρόσβασή του σε όλα τα συστήματα.
18. Ο Ανάδοχος θα διασφαλίσει ότι χρησιμοποιείται κρυπτογράφηση end-to-end σε όλη τη διακίνηση πληροφορίας στο δίκτυο, συμπεριλαμβανομένων του μετρητή προς το MDM, ή του καταναλωτή προς την πλατφόρμα κινητής ή την δικτυακή πλατφόρμα καταναλωτή.
19. Ο Ανάδοχος θα τεκμηριώσει τις υλοποιήσεις της κρυπτογράφησης στο σύστημα AMI/MDM.
20. Ο Ανάδοχος θα πιστοποιήσει ότι έχει υλοποιηθεί κατ΄ ελάχιστον κρυπτογράφηση AES 128bit για τις επικοινωνίες μετρητή προς MDM.
21. Ο Ανάδοχος θα παρέχει τεκμηρίωση σχετικά με τη μεθοδολογία ασφάλειας από άκρο σε άκρο (end-to-end), συμπεριλαμβανομένων του μετρητή προς την οικιακή οθόνη απεικόνισης και του συστήματος AMI/MDM προς τον καταναλωτή.
22. Ο Ανάδοχος θα διασφαλίζει ότι οι μη αναγκαίες υπηρεσίες και προγράμματα που συνοδεύουν το λογισμικό του προμηθευτή αλλά δεν χρησιμοποιούνται από το ΔΕΔΔΗΕ (για οποιονδήποτε λόγο) είναι απενεργοποιημένα ή έχουν απεγκατασταθεί για να μη δημιουργήσουν κάποιο τρωτό σημείο στην ασφάλεια. Ο Ανάδοχος θα τεκμηριώσει αυτές τις υλοποιήσεις.

4 Προστασία Δεδομένων Καταναλωτή

23. Ο Ανάδοχος θα πρέπει να πιστοποιήσει και να επιδείξει συμμόρφωση με το πρότυπο Data Protection Impact Assessment (DPIA) για έξυπνα δίκτυα (Smart Grids) και Συστήματα Έξυπνων Μετρητών (Smart Metering Systems)[1].

5 Τεκμηρίωση Απαιτήσεων Ασφαλείας

24. Ο ανάδοχος θα πρέπει να παραδώσει Μελέτη Αρχιτεκτονικής Ασφάλειας του συστήματος. Στόχος της μελέτης θα είναι η καταγραφή των τεχνικών και λειτουργικών απαιτήσεων και σύμφωνα με αυτές ο σχεδιασμός μιας αρχιτεκτονικής ασφάλειας τόσο σε επίπεδο δικτύου και συστημάτων, όσο και σε επίπεδο Web εφαρμογής. Πρέπει να διασφαλίζεται ότι σημαντικοί παράμετροι ασφάλειας έχουν συμπεριληφθεί στις προδιαγραφές υλοποίησης του συνολικού Πληροφοριακού συστήματος (Security by Design).
25. Ο ανάδοχος πρέπει να αναπτύξει και να εφαρμόσει οδηγούς ασφαλούς παραμετροποίησης (Secure Configuration Guides). Έτσι το σύστημα θα παραμετροποιείται σύμφωνα με κανόνες και βέλτιστες πρακτικές ασφάλειας. Στόχος είναι η ανάπτυξη τεχνικών οδηγών ασφαλούς παραμετροποίησης όλων των δομικών στοιχείων τα οποία απαρτίζουν το Σύστημα και η

[1] http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

υλοποίηση τους σε αυτό πριν από την ένταξη του στην παραγωγική λειτουργία. Συγκεκριμένα, θα πρέπει να αναπτυχθούν και να υλοποιηθούν οδηγοί ασφαλούς παραμετροποίησης κατ' ελάχιστο για:

- Τις βάσεις δεδομένων.
- Τους εξυπηρετητές διαδικτύου (πχ. IIS X.X Secure Configuration guide, Apache X.X Secure Configuration guide etc.)
- Τα λειτουργικά συστήματα τα οποία θα φιλοξενούν τις βάσεις δεδομένων, και τους
- Εξυπηρετητές διαδικτύου.
- Τα Firewalls.

26. Πριν την ένταξη του συστήματος σε παραγωγική λειτουργία πρέπει να πραγματοποιηθούν Penetration Tests, τόσο σε επίπεδο συστήματος και δικτύου (System & Network Penetration Test) όσο και σε επίπεδο εφαρμογής Web (Web Application Penetration Test). Τα προφίλ τα οποία θα προσομοιώνουν τα Penetration Tests είναι τουλάχιστον:
    - System & Network Penetration Test:
        a) Εξωτερικός χρήστης χωρίς δικαιώματα πρόσβασης
        b) Εσωτερικός χρήστης χωρίς δικαιώματα πρόσβασης
        c) Εσωτερικός χρήστης με δικαιώματα πρόσβασης
    - Web Application Penetration Test
        a) Χρήστης με δικαιώματα πρόσβασης
        b) Χρήστης χωρίς δικαιώματα πρόσβασης
27. Ο ανάδοχος πρέπει να σχεδιάσει και να διεξάγει δοκιμές διείσδυσης, σε συνεργασία με ένα ανεξάρτητο φορέα δοκιμών διείσδυσης, ώστε να δοκιμαστεί η συνολική ασφάλεια του συστήματος που παραδίδεται. Ο ΔΕΔΔΗΕ θα εγκρίνει αυτό το σχέδιο. Ο ανάδοχος θα προτείνει 3 ανεξάρτητους πιστοποιημένους φορείς για την εκτέλεση των δοκιμών διείσδυσης, και ο ΔΕΔΔΗΕ θα επιλέξει έναν από αυτούς, για τη διεξαγωγή της τελικής δοκιμής. Ο ανάδοχος είναι υποχρεωμένος να προβεί στις απαραίτητες παρεμβάσεις ώστε να διορθωθούν τυχόν προβλήματα που μπορεί να προκύψουν κατά την εκτέλεση των δοκιμών. Τα αποτελέσματα επιτυχίας των δοκιμών θα πιστοποιηθούν από το φορέα.
28. Ο ανάδοχος θα πρέπει να παραδώσει εγχειρίδιο ασφάλειας του συστήματος, που θα περιγράφει αναλυτικά τις διαδικασίες που πρέπει να τηρούνται, ώστε να μη μειώνεται σε καμία περίπτωση η ασφάλεια του συστήματος.
29. Η ανωτέρω διαδικασία δοκιμών διείσδυσης θα επαναλαμβάνεται σε ετήσια βάση.
30. Η δαπάνη για τις ανωτέρω δοκιμές για το διάστημα της πενταετούς λειτουργίας του συστήματος θα πρέπει να συμπεριληφθεί στην προσφορά του Αναδόχου.

6 Πλαίσιο Ασφάλειας Πληροφορικών Συστημάτων του ΔΕΔΔΗΕ

31. Πέραν των αναφερόμενων στο παρόν τεύχος, θα πρέπει το προσφερόμενο σύστημα να ικανοποιεί το Πλαίσιο Ασφάλειας Πληροφορικών Συστημάτων του ΔΕΔΔΗΕ, σύμφωνα με τα επισυναπτόμενα στο παράρτημα του παρόντος τεύχους:
    - Πρότυπο Κωδικών Πρόσβασης του ΔΕΔΔΗΕ (ΠΑ-1)
    - Πρότυπο Ασφάλειας των Εφαρμογών Πληροφορικής του ΔΕΔΔΗΕ (ΠΑ-2)
    - Πρότυπο Λειτουργίας Πληροφοριακών Συστημάτων του ΔΕΔΔΗΕ (ΠΑ-3)

7 Παράρτημα

Ακολουθούν τα παρακάτω πρότυπα του ΔΕΔΔΗΕ:

- Πρότυπο Κωδικών Πρόσβασης του ΔΕΔΔΗΕ (ΠΑ-1)
- Πρότυπο Ασφάλειας των Εφαρμογών Πληροφορικής του ΔΕΔΔΗΕ (ΠΑ-2)
- Πρότυπο Λειτουργίας Πληροφοριακών Συστημάτων του ΔΕΔΔΗΕ (ΠΑ-3)

ΔΙΑΧΕΙΡΙΣΤΗΣ ΕΛΛΗΝΙΚΟΥ ΔΙΚΤΥΟΥ ΔΙΑΝΟΜΗΣ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ Α. Ε.
ΚΛΙΜΑΚΙΟ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΟΜΕΑΣ ΑΣΦΑΛΕΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΤΥΠΟ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ ΤΗΣ ΔΕΔΔΗΕ Α.Ε.

ΠΑ-1

Έκδοση: **1.0**

ΗΜΕΡΟΜΗΝΙΑ ΈΚΔΟΣΗΣ: 22/05/2013

ΙΣΤΟΡΙΚΌ ΑΛΛΑΓΏΝ

Ημερομηνία	Υπεύθυνος Αλλαγών	Αλλαγές / Προσθήκες (αναφορά συγκεκριμένης ενότητας)	Έγκριση	Αριθμός Έκδοσης	Ημερομηνία Εφαρμογής
22/5/2013	Γ. Μαρεντάκης	Αρχική Έκδοση	Διευθυντής ΚΠΤ	1.0	1/7/2013

ΠΡΟΤΥΠΑ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

1. ΓΕΝΙΚΑ

Οι κωδικοί πρόσβασης (*passwords*) αποτελούν το δεύτερο συστατικό στοιχείο των διαπιστευτηρίων των χρηστών (ταυτότητα χρήστη, κωδικός πρόσβασης), ο συνδυασμός των οποίων είναι μοναδικός για κάθε χρήστη. Αποτελούν σημαντική πλευρά της ασφάλειας των πληροφοριακών συστημάτων και τη βασική γραμμή προστασίας για την πρόσβαση στα πληροφοριακά συστήματα και τις εφαρμογές της ΔΕΔΔΗΕ Α.Ε.

2. ΣΚΟΠΟΣ

Το παρόν κείμενο έχει ως αντικειμενικό σκοπό να θέσει τους κανόνες που πρέπει να τηρούνται για τη δημιουργία των κωδικών πρόσβασης και τα μέτρα που πρέπει να λαμβάνονται από τους χρήστες και τους διαχειριστές των πληροφοριακών συστημάτων της ΔΕΔΔΗΕ Α.Ε. για την προστασία τους.

3. ΠΕΡΙΓΡΑΦΗ

3.1 Οι κωδικοί πρόσβασης αποτελούνται από τουλάχιστον έξι (6) αλφαβητικούς, αριθμητικούς χαρακτήρες και σύμβολα.

3.2 Όλοι οι κωδικοί πρόσβασης των χρηστών πρέπει να αλλάζουν με νέους το αργότερο κάθε έξι (6) μήνες. Οι κωδικοί πρόσβασης χρηστών με υψηλά δικαιώματα (π.χ. διαχειριστές συστημάτων, διαχειριστές βάσεων δεδομένων, διαχειριστές δικτύων) πρέπει να αλλάζουν το αργότερο κάθε τέσσερις (4) μήνες. Γενικά, θα πρέπει να αποφεύγεται η επαναχρησιμοποίηση παλιών κωδικών πρόσβασης.

3.3 Ένας κωδικός πρόσβασης, που δίνεται από το διαχειριστή συστήματος σε κάθε χρήστη, πρέπει να αλλάζει κατά την πρώτη πρόσβαση του χρήστη στο σύστημα.

3.4 Θα παρέχεται η δυνατότητα στους χρήστες από τις εκάστοτε εφαρμογές ή

λειτουργικά συστήματα να αλλάζουν τον κωδικό πρόσβασής τους όποτε αυτό θεωρηθεί απαραίτητο (πάντοτε όμως μετά την διαδικασία αυθεντικοποίησής τους από το σύστημα).

3.5 Η πραγματοποίηση τριών διαδοχικών αποτυχημένων προσπαθειών πρόσβασης θα πρέπει να έχει ως αποτέλεσμα το κλείδωμα του λογαριασμού του χρήστη. Σε αυτή την περίπτωση ο χρήστης δεν θα έχει την δυνατότητα πρόσβασης, έως ότου ο λογαριασμός ενεργοποιηθεί ξανά και παραχωρηθεί νέος κωδικός πρόσβασης.

3.6 Οι κωδικοί πρόσβασης χρηστών δεν πρέπει να συμπεριλαμβάνονται σε ακολουθίες εντολών εισόδου στο σύστημα (*batch logon sequences*). Σε περιπτώσεις όπου επιβάλλεται η χρήση τέτοιων κωδικών, ο διαχειριστής συστήματος που είναι υπεύθυνος για αυτές τις διαδικασίες θα αλλάζει τον κρυπτογραφημένο κωδικό πρόσβασης ανά τακτά χρονικά διαστήματα (π.χ. τουλάχιστον κάθε δύο (2) μήνες). Σε καμία περίπτωση δεν επιτρέπεται οι κωδικοί πρόσβασης χρηστών να είναι ενσωματωμένοι σε κώδικα εφαρμογής.

3.7 Τα αρχεία που περιέχουν κωδικούς πρόσβασης θα διατηρούνται προστατευμένα και κρυπτογραφημένα. Θα πρέπει να γίνεται χρήση μη αντιστρέψιμων τεχνικών κρυπτογράφησης.

3.8 Οι κωδικοί πρόσβασης εισάγονται σε πεδία όπου δεν εμφανίζονται οι χαρακτήρες που πληκτρολογούνται.

3.9 Οι «προκαθορισμένοι» (*default*) κωδικοί πρόσβασης, οι οποίοι συνοδεύουν ορισμένες εφαρμογές ή λειτουργικά συστήματα ή εν γένει δημιουργούνται κατά την εγκατάσταση λογισμικού θα πρέπει να αλλάζουν πριν από την πρώτη χρήση, σύμφωνα με τα ισχύοντα πρότυπα.

3.10 Οι κωδικοί πρόσβασης των χρηστών δίδονται στους χρήστες με ασφαλή τρόπο. Η αποστολή των κωδικών πρόσβασης με τρόπους εύκολα αναγνώσιμους (π.χ. με ανοικτή επιστολή ή με σύστημα ηλεκτρονικής αλληλογραφίας χωρίς χρήση τεχνικών κρυπτογράφησης) δεν επιτρέπεται.

3.11 Οι κωδικοί πρόσβασης των χρηστών είναι αυστηρά προσωπικοί και εμπιστευτικοί και με κανένα τρόπο δεν πρέπει να κοινοποιούνται ή να αποκαλύπτονται σε οποιονδήποτε (ακόμα και στον προϊστάμενο) και να

αναγράφονται οπουδήποτε ή να αποθηκεύονται χωρίς κρυπτογράφηση.

3.12 Οι κωδικοί πρόσβασης δεν πρέπει να είναι εύκολα προβλέψιμοι (π.χ. το μικρό όνομα της/του συζύγου, η αγαπημένη ποδοσφαιρική ομάδα του/της κλπ). Έτσι, οι κωδικοί πρόσβασης συνίσταται να μην περιέχουν στοιχεία όπως:

- Μήνες του χρόνου, ημέρες της εβδομάδας ή οποιοδήποτε άλλο στοιχείο ημερομηνίας.
- Λέξεις οποιασδήποτε γλώσσας.
- Ονόματα οικογένειας, αρχικά ονομάτων, αριθμός μητρώου ή αριθμός κυκλοφορίας οχημάτων, ημερομηνίες γενεθλίων ή άλλα προσωπικά στοιχεία όπως διευθύνσεις ή αριθμοί τηλεφώνου.
- Ταυτότητα χρήστη (*user-id*), ονοματεπώνυμο χρήστη, ταυτότητα ομάδας χρηστών ή άλλος παρόμοιος προσδιοριστής συστημάτων.
- Περισσότερους από δύο διαδοχικούς ίδιους χαρακτήρες.
- Μόνο αλφαβητικούς χαρακτήρες ή μόνο αριθμητικούς χαρακτήρες.
- Οτιδήποτε από τα προηγούμενα με ανάποδη σειρά.
- Οτιδήποτε από τα προηγούμενα στα οποία προηγείται ή ακολουθεί ψηφίο (π.χ., Costas1).
- Χαρακτήρες που βρίσκονται σε διπλανές θέσεις στο πληκτρολόγιο.

3.13 Όταν υπάρχει υποψία ότι ο κωδικός πρόσβασης έχει αποκαλυφθεί, θα πρέπει το περιστατικό να αναφέρεται και να αλλάζει άμεσα ο κωδικός πρόσβασης.

3.14 Αλλαγή κωδικού πρόσβασης που αιτείται ένας χρήστης μπορεί να πραγματοποιηθεί από το αρμόδιο τμήμα μόνο μετά την επιβεβαίωση της ταυτότητας του χρήστη (*user-id*).

3.15 Κατά την ανάπτυξη ή προμήθεια νέων εφαρμογών θα πρέπει να υπάρχει συμμόρφωση με τα παραπάνω πρότυπα κωδικών πρόσβασης.

4. ΑΝΑΦΟΡΕΣ

- BS ISO/IEC 17799 “Information Technology – Code of practice for information security management”.

ΔΙΑΧΕΙΡΙΣΤΗΣ ΕΛΛΗΝΙΚΟΥ ΔΙΚΤΥΟΥ ΔΙΑΝΟΜΗΣ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ Α. Ε.

ΚΛΙΜΑΚΙΟ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΟΜΕΑΣ ΑΣΦΑΛΕΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΤΥΠΟ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΗΣ ΔΕΔΔΗΕ Α.Ε.

ΠΑ-2

Έκδοση: **1.0**

ΗΜΕΡΟΜΗΝΙΑ ΈΚΔΟΣΗΣ: 10/6/2013

ΙΣΤΟΡΙΚΌ ΑΛΛΑΓΏΝ

Ημερομηνία	Υπεύθυνος Αλλαγών	Αλλαγές / Προσθήκες (αναφορά συγκεκριμένης ενότητας)	Έγκριση	Αριθμός Έκδοσης	Ημερομηνία Εφαρμογής
10/6/2013	Γ. Μαρεντάκης	Αρχική Έκδοση	Διευθυντής ΚΠΤ	1.0	1/7/2013

ΠΡΟΤΥΠΟ ΑΣΦΑΛΕΙΑΣ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

1. ΓΕΝΙΚΑ

Κάθε εφαρμογή, προκειμένου να τεθεί σε λειτουργία στο παραγωγικό περιβάλλον της ΔΕΔΔΗΕ Α.Ε., είναι απαραίτητο να έχει ενσωματωμένο έναν ελάχιστο αριθμό προδιαγραφών ασφαλείας οι οποίες αποβλέπουν στην προστασία των εφαρμογών της Επιχείρησης από απώλεια, μη εξουσιοδοτημένη τροποποίηση ή χρήση, καθώς και στη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών αγαθών της ΔΕΔΔΗΕ Α.Ε..

2. ΣΚΟΠΟΣ

Το παρόν κείμενο έχει ως αντικειμενικό σκοπό:

- Να θέσει τους κανόνες ασφαλείας που πρέπει να τηρούνται, προκειμένου μια εφαρμογή να τεθεί σε παραγωγική λειτουργία στο περιβάλλον της ΔΕΔΔΗΕ Α.Ε.
- Να αποτελεί αναπόσπαστο τμήμα κάθε διακήρυξης που αφορά την ανάπτυξη ή προμήθεια εφαρμογών για τη ΔΕΔΔΗΕ Α.Ε. από τρίτους.

3. ΠΕΡΙΓΡΑΦΗ

3.1 **Η ασφάλεια των εφαρμογών ως πρωταρχικό αντικείμενο σχεδιασμού**. Ο σχεδιασμός όλων των εφαρμογών, ιδιαίτερα αυτών με υψηλή ευαισθησία και υψηλές απαιτήσεις διαθεσιμότητας, θα πρέπει να περιλαμβάνει την ασφάλεια στους πρωταρχικούς αντικειμενικούς στόχους του.

3.2 **Διαπιστευτήρια χρηστών:** Τα διαπιστευτήρια των χρηστών για την πρόσβασή τους στις εφαρμογές αποτελούνται από μία ταυτότητα χρήστη (user ID) και έναν κωδικό πρόσβασης (password), ή οποιοδήποτε άλλο στοιχείο (ψηφιακά πιστοποιητικά, tokens, κλπ), το οποίο θα είναι μοναδικό για κάθε χρήστη.

.

3.3 **Σύνθεση της ταυτότητας χρήστη (user ID):** Η ταυτότητα χρήστη θα πρέπει να αποτελείται από τουλάχιστον επτά (7) αλφαριθμητικούς χαρακτήρες, ενώ το μέγιστο μήκος της δεν θα πρέπει να υπερβαίνει τους περιορισμούς που τίθενται από το εκάστοτε σύστημα πληροφορικής.

3.4 **Κωδικοί πρόσβασης (passwords):** Θα πρέπει να υπάρχει πλήρης συμμόρφωση με τα αναφερόμενα στο *«Πρότυπο Κωδικών Πρόσβασης της ΔΕΔΔΗΕ Α.Ε.» (Κωδικός Προτύπου ΠΑ-1).*

3.5 **Αυθεντικοποίηση του συνόλου των διαπιστευτηρίων των χρηστών:** Η ταυτότητα χρήστη και ο κωδικός πρόσβασης θα αυθεντικοποιούνται στο σύνολό τους. Αποτυχία αυθεντικοποίησης θα έχει ως αποτέλεσμα ένα μήνυμα λάθους προς τον χρήστη, το οποίο δεν θα καταδεικνύει ποιο ακριβώς στοιχείο είναι λάθος (π.χ. «Λανθασμένα στοιχεία σύνδεσης» και όχι «Λάθος κωδικός πρόσβασης»).

3.6 **Διατήρηση πληροφοριών χρήστη:** Για κάθε τελικό χρήστη, η εφαρμογή θα πρέπει υποχρεωτικά να διατηρεί τις ακόλουθες πληροφορίες

1. Αριθμός Μητρώου ΔΕΔΔΗΕ
2. Ταυτότητα του χρήστη (User Id)
3. Κωδικός πρόσβασης (Password). Το password θα πρέπει να διατηρείται πάντοτε κρυπτογραφημένο.
4. Επώνυμο χρήστη
5. Όνομα χρήστη
6. Διεύθυνση Εργασίας

7. Τηλέφωνο επικοινωνίας
8. Δικαιώματα πρόσβασης
9. Ημερομηνία τελευταίας αλλαγής του password
10. Ημερομηνία του τελευταίου login του χρήστη.
11. Ημερομηνία διαγραφής του χρήστη: Για λόγους ασφαλείας, η διαγραφή ενός χρήστη είναι λογική και όχι φυσική. Αν ο χρήστης δεν έχει διαγραφεί το πεδίο αυτό θα είναι κενό.
12. Computer name: Το όνομα του σταθμού εργασίας που θα εργάζεται ο χρήστης και το οποίο θα δηλώνεται κατά την αίτηση εισαγωγής του.

Τα πεδία 1, 4, 5, 6, 7 και 12 θα εισάγονται υποχρεωτικά κατά τη διαδικασία εισαγωγής νέου χρήστη.

3.7 **Προστασία των δεδομένων ασφάλειας των εφαρμογών:** Όλα τα δεδομένα ασφάλειας (π.χ. πίνακες χρηστών, πίνακες εξουσιοδοτήσεων) θα πρέπει να είναι απομονωμένα από τα υπόλοιπα τμήματα της εφαρμογής, να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και να τεκμηριώνονται με σαφή τρόπο όλες οι αλληλεπιδράσεις των στοιχείων αυτών με το υπόλοιπο σύστημα. Έτσι, σε περίπτωση που η εφαρμογή βασίζεται σε σχεσιακή βάση, τα παραπάνω στοιχεία θα ανήκουν σε ξεχωριστό schema user με όνομα secuser.

3.8 **Ενεργοποίηση επιλογών βάσει των ρόλων των χρηστών:** Θα πρέπει να περιορίζεται, μέσω τεχνικών προγραμματισμού, η εμφάνιση επιλογών στο μενού της κάθε εφαρμογής ή επιλογών επεξεργασίας, για τις οποίες ο χρήστης δεν έχει την κατάλληλη εξουσιοδότηση εκτέλεσης.

3.9 **Ο ρόλος του διαχειριστή χρηστών.** Πρέπει να προβλέπεται ξεχωριστός ρόλος για τον διαχειριστή χρηστών. Ο διαχειριστής χρηστών πρέπει να έχει τις πιο κάτω δυνατότητες.

– Εισαγωγή/Διαγραφή/Μεταβολή στοιχείων χρήστη

- Απόδοση και μεταβολή δικαιωμάτων πρόσβασης σύμφωνα με την εγκεκριμένη διαδικασία
- Δυνατότητα επιβεβαίωσης των δικαιωμάτων πρόσβασης (μέσω οθόνης και εκτύπωσης) για όλους τους εισηγμένους χρήστες.

Οι παραπάνω διαδικασίες θα υλοποιούνται σε συγκεκριμένη επιλογή του μενού της εφαρμογής

3.10 **Ο ρόλος του υπευθύνου της εφαρμογής.** Πρέπει να προβλέπεται ξεχωριστός ρόλος για τον υπεύθυνο της εφαρμογής. Ο ρόλος αυτός έχει την ευθύνη των παραμετροποιήσεων της εφαρμογής.

3.11 **Απενεργοποίηση μη χρησιμοποιούμενων λογαριασμών χρηστών:** Η εφαρμογή θα πρέπει να δίνει τη δυνατότητα απενεργοποίησης των χρηστών που δεν έχουν χρησιμοποιήσει την εφαρμογή για χρονικό διάστημα μεγαλύτερο των 60 ημερών.

3.12 **Επικύρωση δεδομένων**

Επικύρωση δεδομένων που εισάγονται στην εφαρμογή: Θα πρέπει να χρησιμοποιείται ένας αριθμός ελέγχων / μέτρων προστασίας κατά την εισαγωγή επιχειρησιακών δεδομένων στις εφαρμογές πληροφορικής της ΔΕΔΔΗΕ Α.Ε.. Συγκεκριμένα:

- Ειδικοί έλεγχοι κατά την εισαγωγή δεδομένων που να εντοπίζουν τα ακόλουθα ενδεικτικά λάθη:
  - Εισαγωγή τιμών εκτός του σωστού εύρους
  - Εισαγωγή μη αποδεκτών χαρακτήρων στα ειδικά πεδία
  - Εισαγωγή ελλιπών δεδομένων
- Περιοδική εξέταση του περιεχομένου των κύριων πεδίων εισαγωγής ή των αρχείων δεδομένων της εφαρμογής, για να εξακριβώνεται η εγκυρότητα και η ακεραιότητά τους

– Ανάπτυξη διαδικασιών για την αντιμετώπιση περιπτώσεων εισαγωγής μη έγκυρων δεδομένων

Διασφάλιση εσωτερικής επεξεργασίας δεδομένων: Η επιλογή των κατάλληλων μέτρων προστασίας και ελέγχου για τη διασφάλιση εσωτερικής επεξεργασίας δεδομένων θα βασίζεται στη φύση κάθε εφαρμογής και των επιχειρησιακών επιπτώσεων της αλλοίωσης των δεδομένων. Συγκεκριμένα, προβλέπονται τα ακόλουθα μέτρα προστασίας:

– Έλεγχος και συμφωνία των αρχείων δεδομένων πριν την εισαγωγή τους και μετά την επεξεργασία τους με τη χρήση ειδικών αυτοματοποιημένων διαδικασιών (batch controls)
– Επικύρωση δεδομένων που δημιουργήθηκαν από το σύστημα
– Έλεγχοι της ακεραιότητας των δεδομένων που μεταβιβάστηκαν μεταξύ των κεντρικών και απομακρυσμένων συστημάτων
– Δημιουργία και εξέταση ειδικών αθροισμάτων ελέγχου (hash totals) των αρχείων
– Διαδικασίες αναφοράς λαθών
– Διαδικασίες διόρθωσης λαθών
– Διαδικασίες επανεισαγωγής data
– Διαδικασίες ελέγχου και επανάληψης λειτουργιών
– Διαδικασίες για τον εντοπισμό μη ολοκληρωμένης ή ανεπίκαιρης επεξεργασίας
– Αυτοματοποιημένοι έλεγχοι που να εγγυώνται την ακρίβεια και την αποτελεσματικότητα της πληροφορίας.

Επικύρωση δεδομένων που εξάγονται από την εφαρμογή: Θα χρησιμοποιείται ένας αριθμός ελέγχων / μέτρων προστασίας για την διασφάλιση της εγκυρότητας των επιχειρησιακών δεδομένων που εξάγονται από τις εφαρμογές πληροφορικής της ΔΕΗ. Συγκεκριμένα:

- Ειδικοί έλεγχοι ορθότητας για να εξακριβωθεί ότι τα εξαγόμενα δεδομένα είναι εύλογα
- Συμφωνίες αθροισμάτων των ποσών πριν και μετά την επεξεργασία
- Παροχή των κατάλληλων πληροφοριών στον παραλήπτη των δεδομένων ή στο επόμενο σύστημα επεξεργασίας για να εξακριβωθεί η ακρίβεια και η πληρότητα των δεδομένων
- Reports ώστε να επιβεβαιώνεται η ορθή λειτουργία της εφαρμογής

3.13 **Καταγραφή λαθών (errors).** Τα λάθη/σφάλματα της εφαρμογής θα πρέπει να συγκεντρώνονται σωρευτικά σε ειδικό αρχείο.

3.14 **Ημερολόγια ελέγχου και καταγραφής αλλαγών (log files):** Η ομάδα σχεδιασμού θα πρέπει να λαμβάνει υπόψη την ενσωμάτωση ημερολογίων καταγραφής και παρακολούθησης αλλαγών (logging). Παράδειγμα τέτοιων ημερολογίων αποτελεί η καταγραφή σημαντικών συναλλαγών καθώς και οι ημερομηνίες και ώρες σύνδεσης και αποσύνδεσης των τελικών χρητών . Κατά τον σχεδιασμό, καθορίζεται το επιθυμητό επίπεδο καταγραφής ενεργειών, το οποίο βασίζεται στο βαθμό ευαισθησίας και κρισιμότητας των πληροφοριών που είναι αποθηκευμένες ή επεξεργάζονται από το σύστημα.

3.15 **Παραγόμενες εκτυπώσεις.** Όλες οι παραγόμενες εκτυπώσεις θα πρέπει να περιέχουν :

- Τους κατάλληλους τίτλους
- Το όνομα του προγράμματος επεξεργασίας
- Την ημερομηνία και ώρα παραγωγής

3.16 **Τεκμηρίωση**

Κάθε εφαρμογή πρέπει να συνοδεύεται από την απαραίτητη τεκμηρίωση που αποτελείται από:

- Τεκμηρίωση της εφαρμογής

- Εγχειρίδια για τους χειριστές
- Εγχειρίδια χρηστών

Η τεκμηρίωση μπορεί να θεωρηθεί ως πλήρης όταν κάποιος τρίτος, εκτός αυτών που τη συνέταξαν και τη συντηρούν, μπορεί να λειτουργήσει την εφαρμογή στηριζόμενος απλά και μόνο σε ανάγνωση της.

Τεκμηρίωση της εφαρμογής

Περιέχει όλες τις απαραίτητες πληροφορίες για την πλήρη κατανόηση της λογικής της εφαρμογής. Είναι απαραίτητη σε αναλυτές και προγραμματιστές στο να ελέγχουν αλλαγές και αναθεωρήσεις των προγραμμάτων. Θα πρέπει να περιλαμβάνει:

- Περιγραφή του σκοπού της εφαρμογής.
- Περιγραφή των εργαλείων που χρησιμοποιούνται.
- Λογικά διαγράμματα και πίνακες αποφάσεων.
- Τον κώδικα των προγραμμάτων.
- Το σχήμα και την τεκμηρίωση των βάσεων (αν υπάρχουν).
- Τα σημεία ελέγχου.
- Τα formats των input και output αρχείων.
- Έγκυρα αντίγραφα των εξουσιοδοτήσεων με τις οποίες έχουν γίνει αλλαγές στο πρόγραμμα.

Εγχειρίδια για τους χειριστές

Περιέχει συμβουλές για τους χειριστές σχετικές με την εκτέλεση της συγκεκριμένης εφαρμογής. Βοηθά στην κατανόηση των καθηκόντων τους και καθορίζει τα επί μέρους βήματα. Θα πρέπει να περιλαμβάνει:

- Περιγραφή του σκοπού της εφαρμογής.
- Περιγραφή των πληροφοριών input και output.
- Εντολές για το πρώτο set up.

- Εντολές προς τους χειριστές σχετικές με τη σειρά εκτέλεσης των προγραμμάτων.
- Εντολές για το ανέβασμα και κατέβασμα της εφαρμογής
- Εντολές στους χειριστές σχετικές με παραγόμενα μηνύματα και προγραμματισμένες παύσεις.
- Εντολές σχετικές με την περαιτέρω χρησιμοποίηση του input και τη διάθεση του παραγομένου output.
- Πιθανές ελεγκτικές διαδικασίες που πρέπει να ακολουθήσουν οι χειριστές.
- Εντολές αντιμετώπισης ξαφνικών τεχνικών προβλημάτων.
- Τον προβλεπόμενο συνήθη χρόνο εκτέλεσης.
- Εντολές αντιμετώπισης έκτακτης ανάγκης.

Εγχειρίδιο χρηστών

Περιέχει όλα τα απαραίτητα στοιχεία ώστε κάθε χρήστης να κατανοεί και να αποδέχεται το σύστημα / εφαρμογή. Θα πρέπει να περιλαμβάνει:

- Πλήρη περιγραφή όλων όσων χρησιμοποιεί ο χρήστης για να εκτελεί την εφαρμογή.
- Τους επί μέρους αλλά και τους γενικούς ελέγχους που πρέπει να κάνουν οι χρήστες.
- Τα βήματα της όλης διαδικασίας που πρέπει να ακολουθεί ο χρήστης.
- Τις διαδικασίες αποσύνδεσης και τέλους της εφαρμογής.
- Πλήρη περιγραφή των παραγομένων μηνυμάτων και εντύπων καταστάσεων.
- Την αντίδρασή του σε περιπτώσεις προβλήματος.
- Τι θα πρέπει να αποφεύγει ο χρήστης κατά τη χρήση της εφαρμογής.

Ασφάλεια Τεκμηρίωσης

Κάθε κατηγορία τεκμηρίωσης πρέπει να φυλάσσεται και να συμπληρώνεται όποτε χρειαστεί. Ένας υπεύθυνος (librarian) πρέπει να είναι υπεύθυνος για τον έλεγχο, φύλαξη, συντήρηση και διανομή της γραπτής τεκμηρίωσης. Μόνο εξουσιοδοτημένα άτομα πρέπει να έχουν πρόσβαση και μόνο σε συγκεκριμένο είδος τεκμηρίωσης. Η τεκμηρίωση των προγραμμάτων πρέπει να τυγχάνει ιδιαίτερης προστασίας. Απλές συμβουλές για την ασφάλεια της τεκμηρίωσης είναι:

- Η γραπτή τεκμηρίωση φυλάσσεται σε απροσπέλαστο και πυρασφαλή χώρο.
- Ένα δεύτερο αντίγραφο κάθε είδους τεκμηρίωσης πρέπει να φυλάσσεται σε διαφορετικό κτίριο.
- Κάθε στέλεχος πρέπει να έχει πρόσβαση σε όποιο είδος τεκμηρίωσης απαιτείται να έχει και μόνο.
- Δεν γίνεται καμία διαγραφή ή/και προσθήκη σε τεκμηρίωση χωρίς να έχει κρατηθεί σημείωση σε σχετικό ημερολόγιο.
- Πρέπει να γίνεται αυστηρότατος έλεγχος κατά τη φωτοτύπηση τεκμηρίωσης.
- Επιτυχής χρησιμοποίηση της τεκμηρίωσης θεωρείται όταν αυτή είναι πάντα πλήρως επίκαιρη.

Ορισμός και αρμοδιότητες Υπεύθυνου Εφαρμογής (ΥΕ). Για κάθε εφαρμογή ορίζεται ο Υπεύθυνος Εφαρμογής (Ιδιοκτήτης Εφαρμογής). Ως Υπεύθυνος Εφαρμογής προσδιορίζεται η υπηρεσιακή μονάδα στις αρμοδιότητες της οποίας περιλαμβάνονται τα δεδομένα της εφαρμογής και η ασφάλειά τους. Ο Υπεύθυνος Εφαρμογής:

- Εκδίδει τις λειτουργικές προδιαγραφές τόσο πριν όσο και μετά τη θέση της εφαρμογής σε παραγωγική λειτουργία.
- Πριν τη θέση σε παραγωγική διαδικασία, θα πρέπει να έχει εγκρίνει:

- Τη διαβάθμιση των πληροφοριών ανάλογα με την ευαισθησία και την κρισιμότητά τους (π.χ. εμπιστευτικές, περιορισμένης πρόσβαση κλπ)
- Τα επίπεδα (ρόλους) χρηστών, ανάλογα με τις επιχειρησιακές ανάγκες και τα εργασιακά καθήκοντα.
- Τα δικαιώματα πρόσβασης (αρμοδιότητες) για τον κάθε ρόλο
- Το έντυπο αίτησης για τις προσβάσεις των τελικών χρηστών
- Τη διαδικασία για τη διαχείριση και έγκριση των προσβάσεων των τελικών χρηστών.

Πριν από τη διαδικασία εισόδου τελικών χρηστών στο σύστημα θα πρέπει να έχει αποσταλεί στις Μονάδες η διαδικασία για τη διαχείριση και έγκριση των προσβάσεων των τελικών χρηστών μαζί με το σχετικό έντυπο της αίτησης

3.17 **Διαδικασία backup:** Πριν τη θέση της εφαρμογής σε παραγωγική διαδικασία θα πρέπει να έχουν καθοριστεί οι διαδικασίες λειτουργίας backup / restore / recovery.

3.18 **Προϋποθέσεις για τη θέση της εφαρμογής σε παραγωγική λειτουργία.** Προϋπόθεση για τη θέση μιας εφαρμογής σε παραγωγική λειτουργία είναι η τήρηση και υλοποίηση όλων των προηγουμένων παραγράφων.

3.19 **Επίγνωση απαιτήσεων από εξωτερικούς συνεργάτες**. Όλες οι παραπάνω παράγραφοι αφορούν και τις εφαρμογές των οποίων η προμήθεια γίνεται από εξωτερικούς συνεργάτες.

3.20 **Διαφοροποιήσεις:** Κάθε διαφοροποίηση από τις προηγούμενες παραγράφους επιτρέπεται σε εξαιρετικές περιπτώσεις. Σε κάθε τέτοια περίπτωση οι λόγοι διαφοροποίησης πρέπει να είναι πλήρως τεκμηριωμένοι

4. ΑΝΑΦΟΡΕΣ

❖ «*Πρότυπο κωδικών πρόσβασης της ΔΕΔΔΗΕ Α.Ε (ΠΑ-1)*», Έκδοση 1.0, 22/5/2013.

ΔΙΑΧΕΙΡΙΣΤΗΣ ΕΛΛΗΝΙΚΟΥ ΔΙΚΤΥΟΥ ΔΙΑΝΟΜΗΣ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ Α. Ε.

ΔΙΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΟΜΕΑΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΤΥΠΟ ΛΕΙΤΟΥΡΓΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΤΗΣ ΔΕΔΔΗΕ Α.Ε.

ΠΑ-3

Έκδοση: **1.0**

ΗΜΕΡΟΜΗΝΙΑ ΈΚΔΟΣΗΣ: 23/1/2014

ΙΣΤΟΡΙΚΌ ΑΛΛΑΓΏΝ

Ημερομηνία	Υπεύθυνος Αλλαγών	Αλλαγές / Προσθήκες (αναφορά συγκεκριμένης ενότητας)	Έγκριση	Αριθμός Έκδοσης	Ημερομηνία Εφαρμογής
23/1/2014	Γ. Μαρεντάκης	Αρχική Έκδοση	Διευθυντής ΔΠΛΤ	1.0	1/2/2013

ΠΡΟΤΥΠΟ ΑΣΦΑΛΕΙΑΣ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

1. ΓΕΝΙΚΑ

Για κάθε πληροφοριακό σύστημα, που έχει τεθεί σε λειτουργία στο παραγωγικό περιβάλλον του ΔΕΔΔΗΕ, είναι απαραίτητο να τηρούνται συγκεκριμένες διαδικασίες οι οποίες θα εξασφαλίζουν την προστασία του από μη εξουσιοδοτημένη χρήση και θα διασφαλίζουν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητας των πληροφοριακών αγαθών του ΔΕΔΔΗΕ.

2. ΣΚΟΠΟΣ

Το παρόν κείμενο έχει ως αντικειμενικό σκοπό να θέσει τους κανόνες ασφαλείας και λειτουργίας που πρέπει να τηρούνται, για κάθε πληροφοριακό σύστημα που έχει τεθεί σε παραγωγική λειτουργία στο περιβάλλον του ΔΕΔΔΗΕ.

3. ΠΕΡΙΓΡΑΦΗ

3.1 Τεκμηριωμένες διαδικασίες λειτουργίας

3.1.1 Προϋπόθεση για την παραγωγική λειτουργία μιας εφαρμογής είναι η τήρηση και υλοποίηση του *«Πρότυπου Ασφάλειας των Εφαρμογών Πληροφορικής της ΔΕΔΔΗΕ Α.Ε. (ΠΑ-2)»*.

3.1.2 **Διαδικασίες λειτουργίας**. Οι διαδικασίες λειτουργίας των πληροφοριακών συστημάτων πρέπει να είναι πλήρως τεκμηριωμένες και να διατηρούνται ενημερωμένες. Πρέπει να περιλαμβάνουν σαφείς οδηγίες για τη λεπτομερή εκτέλεση κάθε εργασίας όπως:

- Επεξεργασία και διαχείριση πληροφοριών.
- Χρονικός προγραμματισμός των εργασιών, λαμβάνοντας υπόψη τις αλληλεπιδράσεις με άλλα συστήματα, καθώς και το συντομότερο χρόνο έναρξης και το μέγιστο χρόνο ολοκλήρωσης των εργασιών.

- Οδηγίες για διευθέτηση των λαθών ή άλλων εξαιρέσεων, που μπορούν να προκύψουν κατά τη διάρκεια εκτέλεσης μιας εργασίας, συμπεριλαμβανομένων των περιορισμών στη χρήση του συστήματος.
- Σύνδεσμοι επικοινωνίας για την παροχή εργασιών υποστήριξης σε περίπτωση μη αναμενόμενων λειτουργικών ή τεχνικών δυσκολιών.
- Ειδικές οδηγίες τεκμηρίωσης και διαχείρισης των αποτελεσμάτων/προϊόντων των εργασιών, όπως η χρήση ειδικών επιστολόχαρτων ή η διαχείριση προϊόντων εμπιστευτικού χαρακτήρα.
- Επανεκκίνηση των συστημάτων και διαδικασίες ανάκτησης δεδομένων για να χρησιμοποιηθούν σε περίπτωση διακοπής της λειτουργίας του συστήματος.
- Διαδικασίες διαχείρισης των παραμέτρων λειτουργίας των συστημάτων
- Διαδικασίες αποτροπής εγκατάστασης και χρήσης μη εγκεκριμένου λογισμικού καθώς και λογισμικού χωρίς την κατάλληλη αδειοδότηση.
- Διαδικασίες διαχείρισης της χωρητικότητας, του φόρτου και της απόδοσης των συστημάτων και των δικτύων
- Συνεχής παρακολούθηση των της διαθεσιμότητας των συστημάτων και των δικτύων.
- Διαδικασίες εκκίνησης και κλεισίματος των συστημάτων.
- Επαρκής συντήρηση και τεχνική υποστήριξη των συστημάτων με βάση τις προδιαγραφές και τις ανάγκες τους. Τήρηση πλήρους και ενημερωμένης τεκμηρίωσης για κάθε σύστημα με τα επίσημα εγχειρίδια των εταιριών που προμηθεύουν το υλικό και το λογισμικό των συστημάτων.
- Λήψη και διατήρηση των αντιγράφων ασφαλείας.
- Διαχείριση και προστασία του υπολογιστικού κέντρου

3.1.3 Καταγραφή εξοπλισμού και λογισμικού. Πρέπει να υπάρχει πλήρης και λεπτομερής καταγραφή του μηχανογραφικού εξοπλισμού (κεντρικά συστήματα, εξυπηρετητές, προσωπικοί υπολογιστές, περιφερειακά, δίκτυα και τηλεπικοινωνίες), του αρχιτεκτονικού σχεδιασμού, του χρησιμοποιούμενου λογισμικού, καθώς και του ιστορικού των εκδόσεων, των ενημερώσεων και των αδειών χρήσης.

3.1.4 **Προγραμματισμός εργασιών**. Πρέπει να υπάρχει καταγεγραμμένος ο προγραμματισμός των προς εκτέλεση εργασιών, η καταγραφή των προβλημάτων που προκύπτουν και των ενεργειών που πρέπει να γίνονται σε έκτακτες περιπτώσεις. Η επιτυχής ή μη εκτέλεση των προγραμματισμένων ή και έκτακτων εργασιών θα πρέπει να καταχωρείται σε ειδικό ημερολόγιο, το οποίο και θα φέρει τις υπογραφές του προσωπικού που τις εκτέλεσε. Η εκτέλεση έκτακτων εργασιών θα πρέπει να γίνεται κατόπιν ειδικής έγκρισης.

3.1.5 **Έλεγχος δεδομένων**. Θα πρέπει να γίνεται έλεγχος των δεδομένων, για εξασφάλιση της ορθότητας, της ακεραιότητας και της εμπιστευτικότητας σε όλες τις φάσεις της επεξεργασίας τους. Οι κάθε είδους ασυμφωνίες θα πρέπει να διαπιστώνονται και να αντιμετωπίζονται βάσει καταγεγραμμένων διαδικασιών.

3.1.6 **Καταγραφή συμβάντων.** Πρέπει να υπάρχουν διαδικασίες λεπτομερούς καταγραφής των συμβάντων μη διαθεσιμότητας (επηρεαζόμενα συστήματα, χρονική διάρκεια μη διαθεσιμότητας, αιτία του προβλήματος, τρόπος και χρονική διάρκεια αντιμετώπισης) και άμεση ενημέρωση του Υπεύθυνου Ασφάλειας.

3.1.7 **Υποστήριξη των τελικών χρηστών.** Στην υποστήριξη θα πρέπει να λαμβάνεται υπόψη το είδος των χρηστών και η φύση του προβλήματος που αντιμετωπίζει. Το πλήθος και το είδος των προβλημάτων θα πρέπει να καταγράφονται και να τυγχάνουν στατιστικής επεξεργασίας.

3.1.8 **Αρχεία εξόδου (Output).** Για κάθε εφαρμογή που βρίσκεται σε παραγωγή υπάρχει κατάλογος με τα παραγόμενα αρχεία εξόδου ο οποίος περιέχει πληροφορίες σχετικά με το επίπεδο εμπιστευτικότητας των πληροφοριών που αυτά περιέχουν. Για κάθε ένα από τα παραπάνω αρχεία εξόδου και ανάλογα με το βαθμό εμπιστευτικότητας υπάρχει λίστα η οποία περιέχει τα στοιχεία των αντίστοιχων παραληπτών.

3.1.9 Πρέπει να τηρείται αρχείο για τα μέσα που αποθηκεύουν και διακινούν ευαίσθητα δεδομένα της Επιχείρησης (cartridges, ταινίες,, δισκέτες, CDs, εκτυπώσεις, microfiche κλπ).

3.1.10 Τα αρχεία καταγραφής πρέπει να ενημερώνονται άμεσα σε περιπτώσεις αλλαγών.

3.2 Διαχωρισμός περιβαλλόντων

3.2.1 Το περιβάλλον παραγωγής των συστημάτων είναι πλήρως διαχωρισμένο από τα περιβάλλοντα ανάπτυξης και δοκιμών.

3.2.2 **Μεταφορά προγραμμάτων.** Η μεταφορά προγραμμάτων και δεδομένων από το περιβάλλον παραγωγής στα περιβάλλοντα ανάπτυξης και δοκιμών και αντίστροφα πραγματοποιείται σύμφωνα με καθορισμένη και τεκμηριωμένη διαδικασία από εξουσιοδοτημένα άτομα.

3.2.3 **Χρήση αντιγράφων των δεδομένων παραγωγής κατά τις δοκιμές**. Οι δοκιμές των συστημάτων θα πρέπει να εκτελούνται με αντίγραφα των δεδομένων παραγωγής, από τα οποία έχουν αφαιρεθεί τυχόν ευαίσθητες πληροφορίες. Παράλληλες δοκιμές ή δοκιμές αποδοχής θα εξετάζονται σε συνεργασία με τους εκάστοτε υπεύθυνους πληροφοριακών αγαθών.

3.2.4 **Ελεγχόμενη πρόσβαση σε αποτελέσματα δοκιμών**. Θα πρέπει να πραγματοποιείται έλεγχος πρόσβασης στα αποτελέσματα δοκιμών, στις περιπτώσεις που τα αποτελέσματα αυτά δεν είναι δημόσιας χρήσεως.

3.3 Διαχωρισμός καθηκόντων

3.3.1 Κατά την ανάθεση καθηκόντων που αφορούν κρίσιμες επιχειρησιακές λειτουργίες εφαρμόζεται η αρχή διαχωρισμού καθηκόντων.

3.3.2 Οι αρμοδιότητες πρέπει να είναι διαχωρισμένες σε τέτοια έκταση, έτσι ώστε να μειώνονται οι πιθανότητες για μη εξουσιοδοτημένη χρήση ή κατάχρηση των δυνατοτήτων του συστήματος. Για παράδειγμα, ένας χειριστής δεν θα πρέπει να είναι και προγραμματιστής εφαρμογών ή συστήματος. Επίσης, οι διαχειριστές συστημάτων δεν θα πρέπει είναι και χρήστες επιχειρησιακών εφαρμογών. Ο Πίνακας 1.1 παρέχει με λεπτομέρεια οδηγίες για τον καταμερισμό εργασιών με

βάση την αρχή του διαχωρισμού καθηκόντων, σύμφωνα με πρότυπα του διεθνούς οργανισμού Information Systems Audit and Control Association (ISACA).

Πίνακας 1.1 Πλέγμα ελέγχου διαχωρισμού καθηκόντων

	Αναλυτής Συστημάτων	Προγραμμα-τιστής Εφαρμογών	Χειριστής Συστήματος	Διαχειριστής ΒΔ	Υπεύθυνος Ασφάλειας	Διαχειριστής Συστημάτων
Αναλυτής Συστημάτων			X		X	X
Προγραμματιστής Εφαρμογών			X	X	X	X
Χειριστής Συστήματος	X	X		X	X	X
Διαχειριστής ΒΔ		X	X			X
Υπεύθυνος Ασφάλειας	X	X	X			X
Διαχειριστής Συστημάτων	X	X	X	X	X	

X: Δηλώνει αρμοδιότητες που δεν θα ανατίθενται στο ίδιο άτομο

3.4 Διαχείριση αλλαγών

3.4.1 Προκειμένου να ελαχιστοποιηθεί ο κίνδυνος μη ομαλής λειτουργίας των πληροφοριακών συστημάτων, πρέπει να υπάρχει αυστηρός έλεγχος της εφαρμογής των οποιοδήποτε αλλαγών. Οι διαδικασίες ασφάλειας και ελέγχου των αλλαγών πρέπει να είναι επίσημες και πρέπει να εξασφαλίσουν ότι πρόσβαση στα πληροφοριακά συστήματα δίνεται μόνο σε όσους προβλέπεται με βάση τις πολιτικές ασφάλειας της επιχείρησης. Επειδή οι αλλαγές λογισμικού μπορούν να επηρεάσουν το επιχειρησιακό περιβάλλον, οι διαδικασίες ελέγχου αυτών των αλλαγών πρέπει να περιλαμβάνουν τα παρακάτω:

- Διατήρηση αρχείου των συμφωνηθέντων επιπέδων πρόσβασης.
- Διασφάλιση ότι οι αλλαγές πραγματοποιούνται μόνο από εξουσιοδοτημένους χρήστες.
- Ανασκόπηση διαδικασιών ελέγχων και ακεραιότητας έτσι ώστε να εξασφαλίζεται ότι αυτές δεν παραβιάζονται από τις επικείμενες αλλαγές.
- Προσδιορισμό του λογισμικού υπολογιστών, των πληροφοριών, των βάσεων δεδομένων και του υλικού για τα οποία απαιτούνται τροποποιήσεις
- Λήψη επίσημης έγκρισης για τις επικείμενες αλλαγές πριν αυτές πραγματοποιηθούν.
- Αποδοχή των αλλαγών από τους χρήστες πριν από αυτές εφαρμοστούν.
- Διασφάλιση ότι το σύνολο της τεκμηρίωσης των πληροφοριακών συστημάτων ενημερώνεται με την ολοκλήρωση κάθε μιας από τις πραγματοποιηθείσες αλλαγές ενώ η παλαιά τεκμηρίωση αρχειοθετείται ή καταστρέφεται.
- Διατήρηση αρχείου εκδόσεων (versions) για όλες τις αλλαγές λογισμικού.
- Διατήρηση αρχείου όλων των αιτημάτων αλλαγών.
- Εξασφάλιση ότι τα εγχειρίδια χρηστών και οι διαδικασίες που ορίζουν τον τρόπο εργασίας τους αλλάζουν με τρόπο που ανταποκρίνονται στις νέες αλλαγές.
- Διασφάλιση ότι οι αλλαγές εφαρμόζονται στο σωστό χρόνο και δεν επηρεάζουν την ομαλή λειτουργία της επιχείρησης.

3.5 Διαχείριση αντιγράφων ασφαλείας

3.5.1 Λήψη και διατήρηση αντιγράφων ασφάλειας. Για τα κρίσιμα συστήματα και εφαρμογές πληροφορικής θα πρέπει να λαμβάνονται και να διατηρούνται αντίγραφα ασφάλειας σύμφωνα με σαφείς και τεκμηριωμένες διαδικασίες. Τα αντίγραφα ασφαλείας, ανάλογα με την κρισιμότητα της εφαρμογής, πρέπει να είναι διπλά, εκ των οποίων το ένα θα φυλάσσεται σε διαφορετική τοποθεσία.

3.5.2 Λήψη αντιγράφων ασφάλειας πριν από αναβαθμίσεις / συντήρηση. Θα πρέπει να λαμβάνονται αντίγραφα ασφάλειας από όλες τις εφαρμογές λογισμικού και του

λογισμικού συστήματος που μπορούν να επηρεαστούν από την πραγματοποίηση μιας αναβάθμισης ή συντήρησης.

3.5.3 Εξαμηνιαία επισκόπηση αποθηκευμένων αντιγράφων ασφάλειας εκτός κύριας τοποθεσίας: Θα πρέπει να γίνεται επιθεώρηση ανά τακτά χρονικά διαστήματα (τουλάχιστον ανά εξάμηνο) σε όλα τα αποθηκευμένα αντίγραφα ασφάλειας σε ταινία ή άλλο μέσο εκτός κύριας τοποθεσίας.

3.6 Διαχείριση και ασφάλεια αποθηκευτικών μέσων

3.6.1 **Λήψη εξουσιοδότησης για την απομάκρυνση αποθηκευτικού μέσου**. Η απομάκρυνση ενός αποθηκευτικού μέσου (tapes, tape drives, cartridges, hard disks κ.α.) από το χώρο του κέντρου πληροφορικής θα γίνεται μόνο κατόπιν σχετικής έγκρισης.

3.6.2 **Ασφάλεια αποθηκευτικών μέσων.** Αποθηκευτικά μέσα που περιέχουν δεδομένα ή λογισμικό (δισκέτες, ταινίες, CDs, κλπ.) θα διατηρούνται σε ασφαλή θέση, όπου δεν επιτρέπεται η πρόσβαση σε άτομα που δεν έχουν ευθύνη για την φύλαξή τους.

3.6.3 **Διαγραφή δεδομένων από ηλεκτρονικά ή φυσικά αποθηκευτικά μέσα**. Τα ηλεκτρονικά αρχεία δεδομένων θα διαγράφονται από τα αποθηκευτικά μέσα, πριν αυτά πωληθούν, παραχωρηθούν ή απορριφθούν, έτσι ώστε τα διαγραμμένα δεδομένα να μην μπορούν να ανακτηθούν με σύγχρονα εργαλεία υλικού και λογισμικού. Επίσης, τα φυσικά αρχεία, φάκελοι, έγγραφα που περιέχουν ευαίσθητες πληροφορίες και δεδομένα θα καταστρέφονται με τρόπο που οι πληροφορίες αυτές να μην είναι ανακτήσιμες.

3.6.4 **Προστασία ευαίσθητων πληροφοριών κατά την απόσυρση εξοπλισμού πληροφορικής.** Τα δεδομένα είναι πιθανόν να εκτεθούν από μη προσεκτική διάθεση εξοπλισμού πληροφορικής. Όλα τα μηχανήματα που περιέχουν αποθηκευτικά μέσα (π.χ. σκληροί δίσκοι) θα ελέγχονται για να εξασφαλιστεί ότι δεν περιέχουν ευαίσθητες πληροφορίες ή λογισμικό, τα οποία έχουν διαγραφεί ή απεγκατασταθεί πριν την διάθεση ή καταστροφή των μηχανημάτων.

3.6.5 Αναγκαιότητα εξουσιοδότησης για μετακίνηση υπολογιστών και υλικού της Επιχείρησης. Μη εξουσιοδοτημένη μετακίνηση των υπολογιστών ή άλλου υλικού του ΔΕΔΔΗΕ θα θεωρείται κλοπή. Οι υπολογιστές, εκτός των φορητών, επιτρέπεται να μετακινούνται για επιχειρησιακούς σκοπούς μόνο και εφόσον χορηγείται η απαραίτητη εξουσιοδότηση.

4. ΑΝΑΦΟΡΕΣ

❖ «*Πρότυπο Ασφάλειας των Εφαρμογών Πληροφορικής της ΔΕΔΔΗΕ Α.Ε. (ΠΑ-2)*», Έκδοση 1.0, 10/6/2013.