Εγχειρίδιο Διαδικασιών Τμήματος Μηχανογράφησης

ΣΥΝΕΔΡΙΑΣΗ Δ.Σ. 35η/18-09-2017

T.E.A.Y.E.T.

ΣΕΠΤΕΜΒΡΙΟΣ 2017

Περιεχόμενα

Εισαγωγή

Ο ρόλος του Τμήματος Μηχανογράφησης είναι η ανάπτυξη, υποστήριξη και ο συντονισμός των λειτουργιών όλων των εφαρμογών πληροφορικής σε κεντρικό επίπεδο καθώς και η διαχείριση έργων και σχέσεων με τρίτους στους οποίους έχει ανατεθεί η ανάπτυξη εφαρμογών ή/και προμήθεια εξοπλισμού.

Οι κύριες εργασίες του Τμήματος είναι:

- Παρακολούθηση και αποκατάσταση Hardware & Software.
- Παρακολούθηση και αποκατάσταση δικτύου.
- Παρακολούθηση και ενημέρωση mail server.
- Παρακολούθηση και διαρκής ενημέρωση της ιστοσελίδας.
- Παρακολούθηση καλής λειτουργίας και ολοκλήρωσης Backup.
- Συνεργασία με εταιρίες κατασκευής προγραμμάτων για διορθώσεις και βελτιώσεις.
- Συλλογή αιτημάτων από τους χρήστες και προώθηση στις κατά περίπτωση εταιρίες.
- Ανάπτυξη νέων εφαρμογών.
- Συντήρηση εφαρμογών.
- Παρακολούθηση όλων των περιφερειακών συστημάτων.
- Παρακολούθηση νέων τεχνολογιών και προτάσεις προς τη Διοίκηση.

Το Τμήμα Μηχανογράφησης είναι υπεύθυνο για τη σωστή λειτουργία του δικτύου και των συστημάτων της μηχανογράφησης. Επιπλέον, ελέγχει το σύνολο των μέσων (υλικό, λογισμικό, διαδικασίες) και των δραστηριοτήτων ώστε να εξασφαλιστεί η καλή λειτουργία του και να επιτευχθεί η μέγιστη δυνατή απόδοση του. Λόγω της σύνθετης λειτουργίας του διατηρεί άμεσες σχέσεις και διαδραστικές λειτουργίες με όλα τα κύρια τμήματα του Ταμείου, προκειμένου να διασφαλίζεται η απρόσκοπτη, άρτια και σύγχρονη μηχανογραφική υποστήριξη όλων των λειτουργιών του.

1. Διαδικασία διαχείρισης πληροφοριών και πληροφοριακών συστημάτων

1.1.Πληροφοριακά Συστήματα

Το Ταμείο χρησιμοποιεί τα παρακάτω πληροφοριακά συστήματα και τις επιμέρους εφαρμογές για την διαχείριση των λειτουργιών του:

- Πληροφοριακό Σύστημα ΗΔΙΚΑ
  - Εφαρμογή τήρησης μητρώου εργαζομένων
  - Εφαρμογή τήρησης μητρώου Εργοδοτών
  - Εφαρμογή καταχώρησης / υπολογισμού εισφορών
  - Εφαρμογή τήρησης μητρώου συνταξιούχων
  - Έλεγχος ισοζυγίων εργοδοτών
- Πληροφοριακό Σύστημα καρτελών ”ΤΡΙΓΚΑΣ”
  - Τήρηση ψηφιοποιημένων καρτελών εργοδοτών
  - Τήρηση ψηφιοποιημένων καταστάσεων ασφαλισμένων
- Πληροφοριακό Σύστημα πρωτοκόλλησης DBS
  - Εφαρμογή ηλεκτρονικής πρωτοκόλλησης
- Πληροφοριακό Σύστημα Γενικής Λογιστικής DBS
  - Εφαρμογή Λογιστηρίου
- Πληροφοριακό Σύστημα Λογιστικής Αξιογράφων AIS
  - Υπολογισμός αποδόσεων χαρτοφυλακίου
  - Αποτίμηση μεριδίων
- Πληροφοριακό Σύστημα καταγραφής κλήσεων AMITEL
  - Εφαρμογή καταγραφής/ηχογράφησης κλήσεων
- Ενιαίο Πληροφοριακό Σύστημα opus **IOL**
  - Εφαρμογή υπολογισμού εισφορών
  - Απόδοση μεριδίων κεφαλαίου
  - Τήρηση Μητρώου εργοδοτών
  - Τήρηση Μητρώου Ασφαλισμένων
  - Εφαρμογή ελέγχου ισοζυγίων εργοδοτών
  - Διαβαθμισμένη πρόσβαση χρηστών μέσω διαδικτύου (portal)
  - Αυτόματη δημιουργία προστίμων
  - Αυτόματος υπολογισμός εισφορών
- Πληροφοριακό Σύστημα Debian
  - Αυτόματος / κατά περίπτωση συγχρονισμός με ΗΔΙΚΑ
  - Καταμέτρηση μεριδίων
  - Έλεγχο ισοζυγίων εργοδοτών
  - Έλεγχο μητρώου και πληρωμών συντάξεων
  - Εξαγωγή στατιστικών και συνόλων
  - Έλεγχος ορθότητας ηλεκτρονικών αρχείων εισφορών και απογραφικών δελτίων
  - Δημιουργία βεβαιώσεων εισφορών και συντάξεων

1.2.Ασφάλεια Πληροφοριών - Εμπιστευτικά

Όλες οι πληροφορίες του Ταμείου (προσωπικά δεδομένα ασφαλισμένων, κινήσεις λογαριασμών, αναφορές προς την Διοίκηση, βάσεις δεδομένων, λίστες ηλεκτρονικού ταχυδρομείου, εσωτερικό λογισμικό, τεκμηρίωση υπολογιστών, κωδικοί πρόσβασης κ.λπ.) χρησιμοποιούνται μόνο για τους σκοπούς που έχει ορίσει η Διοίκηση. Η χρήση των πληροφοριών αυτών για οποιοδήποτε άλλο σκοπό δεν επιτρέπεται παρά μόνο μετά από ειδική άδεια και έγκριση της Διοίκησης του Ταμείου.

Αποθηκευτικά μέσα (σκληροί δίσκοι, CD, DVD, κ.τ.λ.), εκτυπώσεις, εγχειρίδια και έντυπα γενικότερα που περιλαμβάνουν ευαίσθητες πληροφορίες, φυλάσσονται σε κατάλληλους χώρους και δεν αφήνονται εκτεθειμένα ιδιαίτερα μετά τη λήξη του ωραρίου εργασίας. Με αυτό τον τρόπο οι εμπιστευτικές πληροφορίες προστατεύονται τόσο από προσπάθειες μη εξουσιοδοτημένης πρόσβασης, όσο και από ακούσια καταστροφή. Η προστασία των πληροφοριών διενεργείται βάσει της κρισιμότητας τους.

Τα αποθηκευτικά μέσα που περιέχουν ευαίσθητες/κρίσιμες πληροφορίες που δεν χρειάζονται πλέον, είτε καταστρέφονται φυσικά, είτε διαγράφονται με κάποια ασφαλή διαδικασία. Ειδικότερα, τα έγγραφα που περιλαμβάνουν ευαίσθητες πληροφορίες, όπως ευαίσθητα δεδομένα ασφαλισμένων, καταστρέφονται με τη χρήση καταστροφέων εγγράφων.

Συγκεκριμένα, κάθε εργαζόμενος ο οποίος έχει στη διάθεσή του εμπιστευτικές πληροφορίες οφείλει:

- Να τηρεί εχεμύθεια και να κάνει χρήση των πληροφοριών μόνο για εξουσιοδοτημένους σκοπούς.
- Να μη χρησιμοποιεί τέτοιες πληροφορίες για προσωπικό όφελος, πριν αυτές δημοσιοποιηθούν.
- Να μην κοινοποιεί ή ανακοινώνει τέτοιες πληροφορίες σε συναδέλφους, φορείς ή τρίτους εκτός εάν αυτά τα άτομα είναι ειδικά εξουσιοδοτημένα να λαμβάνουν αυτές τις πληροφορίες.

Εάν ένας εργαζόμενος δεν είναι βέβαιος πότε μπορεί να ενεργεί ή να αποκαλύπτει ξεκάθαρα πληροφορίες τις οποίες έχει, συμβουλεύεται τον Προϊστάμενο στον οποίο αναφέρεται.

Δικαίωμα πρόσβασης σε πληροφορίες με διαβάθμιση «ΕΜΠΙΣΤΕΥΤΙΚΕΣ» και άνω δίνεται μόνο από τον Διευθυντή του Ταμείου.

1.3. Χρήση Λογισμικού

Το Ταμείο χρησιμοποιεί μόνο εξουσιοδοτημένο λογισμικό με συγκεκριμένες και εγκεκριμένες προδιαγραφές και δυνατότητες. Μη εξουσιοδοτημένο λογισμικό, δηλαδή οποιοδήποτε λογισμικό δεν έχει εγκατασταθεί από εξουσιοδοτημένο προσωπικό του Τμήματος Μηχανογράφησης, δεν χρησιμοποιείται ή αποθηκεύεται σε πληροφοριακά συστήματα ή προσωπικούς υπολογιστές του Ταμείου καθώς ελλοχεύει ο κίνδυνος βλάβης ή αλλοίωσης των πληροφοριών και των συστημάτων του.

Οι χρήστες μεταχειρίζονται πάσης φύσης λογισμικό σύμφωνα με τους όρους της Άδειας Χρήσης του. Συγκεκριμένα, απαγορεύεται κάθε είδους χρήση, εγκατάσταση ή αντιγραφή λογισμικού που δεν είναι σύμφωνη με την Άδεια Χρήσης. Επιπλέον, το προσωπικό θεωρεί ότι κάθε λογισμικό υπόκειται σε δικαιώματα δημιουργού, εκτός αν υπάρχει συγκεκριμένη δήλωση που εκφράζει σαφώς το αντίθετο.

Απαγορεύεται η οποιαδήποτε εγκατάσταση/μεταβολή λογισμικού ή εξοπλισμού σε Πληροφοριακό Σύστημα του Ταμείου χωρίς την προηγούμενη έγκριση του Τμήματος Μηχανογράφησης. Οποιεσδήποτε προσθήκες κρίνονται απαραίτητες εγκρίνονται από τον Υπεύθυνο του Τμήματος. Πιο αναλυτικά, δεν επιτρέπεται βάσει των χορηγούμενων προσβάσεων ασφαλείας, η εγκατάσταση λογισμικού από τους απλούς χρήστες. Ως απλοί χρήστες θεωρούνται όλοι οι εργαζόμενοι του Ταμείου. Το Τμήμα Μηχανογράφησης χρησιμοποιεί τους κωδικούς administrator μόνο όταν κριθεί απαραίτητο.

Το Ταμείο στα πλαίσια της προμήθειας λογισμικού από Εξωτερικούς Προμηθευτές, διασφαλίζει και την ανάπτυξη και συντήρηση των λογισμικών που χρησιμοποιεί. Επίσης, ανάλογα με τις ανάγκες του και την ιλιγγιώδη ανάπτυξη της τεχνολογίας, προσαρμόζει κατάλληλα τα πληροφοριακά του συστήματα έτσι ώστε να ανταποκρίνονται στους στόχους του και να προωθούν την εύρυθμη λειτουργία του.

1.4. Πρόσβαση Πληροφοριακών Συστημάτων

Ο κάθε χρήστης έχει μοναδικό κωδικό πρόσβασης στον υπολογιστή του ο οποίος αλλάζει κάθε τρίμηνο βάσει συγκεκριμένων κανόνων πολυπλοκότητας για λόγους ασφαλείας. Για την πρόσβαση στα αρχεία του server υπάρχουν συγκεκριμένα access rights ανά επίπεδο υπαλλήλου και ανά επίπεδο Τμήματος, ενώ για την πρόσβαση σε αρχεία άλλου τμήματος λαμβάνεται ειδική άδεια από τη Διεύθυνση, για το λόγο και την αναγκαιότητα της πρόσβασης.

Απαγορεύεται κάθε προσπάθεια παράκαμψης των διαφόρων μηχανισμών ελέγχου-προστασίας και ασφάλειας που έχει και που θα υλοποιήσει το Ταμείο στα πληροφοριακά και δικτυακά του συστήματα.

Δεν επιτρέπεται στο προσωπικό να χρησιμοποιεί τα πληροφοριακά συστήματα του Ταμείου για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε οποιαδήποτε άλλα πληροφοριακά συστήματα ή να βλάπτει, μεταβάλλει ή να εμποδίζει τις λειτουργίες αυτών. Απαγορεύεται ρητά στο προσωπικό να υποκλέπτει ή με οποιοδήποτε άλλο τρόπο να ανακαλύπτει κωδικούς πρόσβασης, κρυπτογραφικά κλειδιά ή οποιοδήποτε άλλο εγκατεστημένο μηχανισμό ελέγχου πρόσβασης ο οποίος θα μπορούσε να του επιτρέψει μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά συστήματα τρίτων.

Απαγορεύεται ρητά η χρήση πληροφοριακών συστημάτων του Ταμείου από τρίτους, συμπεριλαμβανομένων μελών οικογενείας εργαζομένων.

Επιτρέπεται η χρήση των πληροφοριακών συστημάτων του Ταμείου για προσωπικούς σκοπούς, αλλά πάντοτε μέσα στο πλαίσιο που ορίζουν οι σχετικές πολιτικές και διαδικασίες ασφάλειας και κυρίως για υπηρεσιακούς λόγους. Περιστασιακή χρήση των πληροφοριακών συστημάτων για προσωπικούς λόγους επιτρέπεται μόνο αν:

- Δε προκαλεί οποιασδήποτε μορφής απώλεια στο Ταμείο.
- Δε στοχεύει σε επίτευξη προσωπικού οφέλους του εργαζόμενου ή άλλης επιχειρηματικής οντότητας πλην του Ταμείου (εμπλοκή σε προσωπικές επιχειρηματικές δραστηριότητες του εργαζομένου, επιχειρήσεις με τις οποίες ο εργαζόμενος έχει οποιαδήποτε σχέση κερδοσκοπική ή μη κ.τ.λ.)
- Δεν καταναλώνει σημαντικό ποσοστό των πόρων των συστημάτων.
- Δεν επηρεάζει την παραγωγικότητα των εργαζομένων.
- Δεν παρενοχλεί συναδέλφους.
- Δεν αντίκειται στην παρούσα και σε οποιαδήποτε άλλη πολιτική του Ταμείου.

1.5. Προστασία από ιούς

Το Ταμείο διαθέτει κατάλληλο εγκεκριμένο λογισμικό για την προστασία από ιούς για όλες τις υπηρεσίες και εφαρμογές που προσφέρει στους χρήστες. Το λογισμικό ενημερώνει αυτόματα τη βάση δεδομένων με τις πρόσφατες υπογραφές των ιών (virus definitions). Το εν λόγω λογισμικό επιτρέπει τον καθορισμό προγραμματισμένων ελέγχων στους δίσκους του συστήματος, σε συγκεκριμένη ημερομηνία και ανά τακτά χρονικά διαστήματα. Διενεργεί καθημερινούς ελέγχους σε αρχεία που είναι αποθηκευμένα στον διακομιστή, στα Πληροφοριακά Συστήματα, στο δίκτυο, στα μηχανήματα του Ταμείου και σε οποιαδήποτε μονάδα βοηθητικής μνήμης. Τα αρχεία αυτά μπορεί να είναι αρχεία δεδομένων, αρχεία συστήματος ή αρχεία εφαρμογών. Επιπρόσθετα, το λογισμικό του Ταμείου ελέγχει τα εισερχόμενα και εξερχόμενα μηνύματα ηλεκτρονικής αλληλογραφίας για την ύπαρξη ιών (στα συνημμένα αρχεία). Επιπλέον, ο Υπεύθυνος του Τμήματος Μηχανογράφησης ελέγχει την αναφορά καταγεγραμμένων συμβάντων και προβαίνει στις απαραίτητες ενέργειες.

Η προστασία απέναντι στο κακόβουλο λογισμικό βασίζεται στην ενημέρωση του προσωπικού για την ασφάλεια του Ταμείου, τα κατάλληλα δικαιώματα προσπέλασης και τους μηχανισμούς διαχείρισης αλλαγών στο σύστημα.

1.6. Διαδικασία Τήρησης Αντιγράφων Ασφαλείας

Στο server τηρούνται back up σε καθημερινή βάση από κάθε τμήμα του Ταμείου και η πρόσβαση σε αυτά επιτρέπεται μόνο στο Τμήμα Μηχανογράφησης. Η δημιουργία αντιγράφων ασφαλείας των αρχείων στοχεύει στην προστασία τους από τη μόνιμη απώλεια ή αλλαγή τους σε περίπτωση ακούσιας διαγραφής, επίθεσης από ιό ή σε περίπτωση αστοχίας του λογισμικού ή του υλικού. Εάν συμβεί κάτι από τα παραπάνω, το Ταμείο, έχοντας αντίγραφα ασφαλείας, είναι σε θέση να κάνει επαναφορά των δεδομένων του. Τα αντίγραφα εξυπηρετούν σε πολύ μεγάλο βαθμό την ασφάλεια των δεδομένων και των συστημάτων του Ταμείου, καθώς πολλά από τα δεδομένα αυτά είναι ιδιαίτερα ευαίσθητα και είναι πολύ σημαντική η προστασία του απορρήτου τους.

Το Ταμείο διαθέτει στις κτιριακές του εγκαταστάσεις 4 (τέσσερις) servers με κοινό χώρο αποθήκευσης, οι οποίοι εξυπηρετούν την ασφαλή αποθήκευση των δεδομένων που διαχειρίζονται οι χρήστες καθώς τα δεδομένα αποθηκεύονται και σε αυτές τις μονάδες. Οι servers φιλοξενούν εννέα (9) εικονικούς. Για την ασφαλή λειτουργία των εν λόγω μονάδων, υπάρχει το V-Sphere πρόγραμμα το οποίο παρακολουθεί τη φυσική κατάσταση των server προκειμένου να διασφαλίζεται η ορθή λειτουργία τους.

Ο Υπεύθυνος του Τμήματος Μηχανογράφησης έχει την ευθύνη για την επισκόπηση της διενέργειας backup των κρίσιμων αρχείων στο τέλος κάθε εργάσιμης ημέρας. Τα αρχεία αποθηκεύονται στους servers αλλά και σε ειδικά tapes.

Λόγω του ότι τα back up tapes πρέπει να έχουν καταγεγραμμένα εξωτερικά κρίσιμα στοιχεία τα οποία διευκολύνουν στην αναγνώρισή τους, εξωτερικά αναγράφονται στοιχεία όπως ημερομηνία και περιγραφή του περιεχομένου.

Τα back up tapes των συστημάτων φυλάσσονται σε Τραπεζική Θυρίδα κατόπιν απόφασης του Διοικητικού Συμβουλίου. Πρόσβαση στην Τραπεζική Θυρίδα έχει ο Διευθυντής του Ταμείου και ένα μέλος του Δ.Σ..

Για τα λειτουργικά συστήματα, το λογισμικό, τα δεδομένα και τις εφαρμογές τηρούνται τουλάχιστον τέσσερις γενιές εφεδρικών αντιγράφων σε tapes:

- Μία σε ημερήσια βάση, κάθε βράδυ (hot-spare back up), τα οποία φυλάσσονται για 15 ημέρες.
- Το δεύτερο αντίγραφο τηρείται σε εβδομαδιαία βάση.
- Το τρίτο αντίγραφο τηρείται σε μηνιαία βάση.
- Το τέταρτο αντίγραφο τηρείται σε ετήσια βάση.

Για τις υπόλοιπες εφαρμογές, λογισμικά πακέτα και εφαρμογές που υπάρχουν σε τοπικούς δίσκους, προσωπικούς υπολογιστές, “laptops” κ.τ.λ. η ευθύνη επαρκούς τήρησης και φύλαξης αντιγράφων ανήκει στο χρήστη που σε συνεργασία με τον Υπεύθυνο του Τμήματος Μηχανογράφησης του Ταμείου εξασφαλίζει τουλάχιστον μια γενιά αντιγράφων σε usb stick ή άλλο μαγνητικό μέσο που φυλάσσονται σε ασφαλές σημείο.

Με ευθύνη του Υπευθύνου του Τμήματος Μηχανογράφησης διενεργείται ανά τακτά χρονικά διαστήματα έλεγχος της δυνατότητας τους συστήματος για επαναφορά των αρχείων που χάνονται, στην αρχική τους κατάσταση (restore). Σύμφωνα με τα αποτελέσματα των εν λόγω ελέγχων, ο χρόνος επαναφοράς των αρχείων στην αρχική τους κατάσταση ανέρχεται στις 24 ώρες.

1.7. Ζητήματα προσωπικού

Οι υπάλληλοι του Ταμείου υποχρεούνται να μην εκθέτουν, με τις ενέργειες ή τις παραλείψεις τους, σε κινδύνους το Πληροφοριακό Σύστημα και να συμβάλλουν στην αντιμετώπιση των σχετικών κινδύνων. Υποχρεούνται επίσης να προστατεύουν τα συνθηματικά τους και να μην τα αποκαλύπτουν σε κανέναν, να μη χρησιμοποιούν αναξιόπιστο λογισμικό που λαμβάνουν με το ηλεκτρονικό ταχυδρομείο ή που αποκτούν από το διαδίκτυο, και να μην χρησιμοποιούν πειρατικό ή άλλο παράνομο λογισμικό.

Το Ταμείο επιλέγει, σε θέσεις που είναι σημαντικές για την ασφαλή λειτουργία του πληροφοριακού του συστήματος, προσωπικό με κατάλληλα τυπικά και ουσιαστικά προσόντα.

2. Διαδικασία προμήθειας, υποστήριξης και ανάπτυξης περιφερειακού εξοπλισμού

2.1. Παραλαβή Αίτησης

Το Τμήμα Μηχανογράφησης παραλαμβάνει από τις λοιπές Διευθύνσεις / Τμήματα του Ταμείου αιτήματα (προφορικά ή μέσω e-mail) για την προμήθεια νέου εξοπλισμού / προγράμματος. Επίσης, ο εντοπισμός της ανάγκης ενδέχεται να διενεργηθεί και από τον Υπεύθυνο του Τμήματος Μηχανογράφησης και αναλόγως απευθύνεται στον Διευθυντή του Ταμείου για έγκριση με κοινοποίηση στο Τμήμα Λογιστηρίου για την προμήθεια νέου εξοπλισμού / προγράμματος. Η αίτηση προμήθειας εγκρίνεται από τον Υπεύθυνο του Τμήματος Μηχανογράφησης και εισηγείται από τον Διευθυντή του Ταμείου στο Διοικητικό Συμβούλιο προς τελική έγκριση.

2.2. Διενέργεια παραγγελίας

Η αίτηση εξετάζεται ως προς τη συμμόρφωσή της με το πλαίσιο οδηγιών του Ταμείου για την προμήθεια νέου εξοπλισμού/ προγράμματος και αξιολογούνται οι ανάγκες τις οποίες καλείται να καλύψει η προμήθεια του εξοπλισμού/προγράμματος. Στην περίπτωση έγκρισης της αίτησης από τη Διεύθυνση του Ταμείου βάσει του ποσού της κάθε δαπάνης, καθορίζονται οι προδιαγραφές του εξοπλισμού (τελική σύνθεση, απαιτούμενα τεχνικά χαρακτηριστικά) από το Τμήμα Μηχανογράφησης. Στη συνέχεια, ακολουθείται η αντίστοιχη διαδικασία επιλογής και τελικά ετοιμάζεται το Δελτίο Παραγγελίας ή e-mail το οποίο και αποστέλλεται στον προμηθευτή.

2.3. Παραλαβή υλικών – Εγκατάσταση εξοπλισμού

2.3.1. Υλικά και εξοπλισμός

Ο Υπεύθυνος του Τμήματος Μηχανογράφησης είναι αρμόδιος για την παραλαβή και τον έλεγχο των υλικών που έχουν παραγγελθεί. Ελέγχει την ποσότητα, την ποιότητα και την τιμή των παραληφθέντων υλικών σύμφωνα με τις προδιαγραφές και το Δελτίο Παραγγελίας. Κατόπιν του σχετικού ελέγχου, το τιμολόγιο υπογράφεται και προωθείται στο Τμήμα Λογιστηρίου για καταχώρηση.

2.3.2. Έλεγχος λειτουργίας εξοπλισμού και Λογισμικού

Αφού ολοκληρωθούν οι ενέργειες εγκατάστασης και ρυθμίσεων υλικού και λογισμικού, ακολουθείται από τον Υπάλληλο του Τμήματος Μηχανογράφησης ο έλεγχος λειτουργίας. Στη συνέχεια, καταγράφει τον νέο εξοπλισμό πληροφορικής στις λίστες του μηχανογραφικού εξοπλισμού του Ταμείου.

2.4. Ανάπτυξη Πληροφοριακών Συστημάτων

Ο Υπεύθυνος του κάθε Τμήματος έχει την ευθύνη για τον εντοπισμό και την έγκαιρη προώθηση στο Τμήμα Μηχανογράφησης των αναγκών του τμήματός του για μηχανογραφική υποστήριξη. Παράλληλα, το Τμήμα Μηχανογράφησης παρακολουθεί τις εξελίξεις σχετικά με τις εφαρμογές που υποστηρίζουν τις δραστηριότητες του Ταμείου, έτσι ώστε να διασφαλίζει την καλύτερη δυνατή μηχανογραφική υποστήριξή του.

Ο Υπεύθυνος του Τμήματος Μηχανογράφησης είναι αρμόδιος για την αξιολόγηση της αναγκαιότητας και της σημαντικότητας του κάθε αιτήματος και τη λήψη των κατάλληλων ενεργειών ικανοποίησής του, στον καλύτερο δυνατό χρόνο.

Τα κυριότερα κριτήρια της αξιολόγησης των αιτημάτων είναι τα εξής:

- Τα προβλήματα και οι δυσκολίες που συνεπάγεται η μη εκπλήρωση της ανάγκης.
- Τα οφέλη που θα προκύψουν από την ανάπτυξη ή την αναπροσαρμογή της κάθε εφαρμογής.
- Τα τμήματα και οι δραστηριότητες που αφορά η συγκεκριμένη εφαρμογή.
- Το κόστος αγοράς ή ανάπτυξης της μηχανογραφικής εφαρμογής.
- Η συμβατότητα του απαιτούμενου προγράμματος ή εφαρμογής με τα υφιστάμενα προγράμματα του Ταμείου.

Κατά τη διαδικασία της ανάπτυξης των πληροφοριακών συστημάτων, ο Υπεύθυνος του Τμήματος Μηχανογράφησης λαμβάνει μέρος στα ακόλουθα στάδια ως εξής:

- Κατά τη φάση της μελέτης, καταγράφει αναλυτικά τις ανάγκες των χρηστών όσον αφορά το λογισμικό καθώς και τα προαπαιτούμενα.
- Κατά τη φάση της ανάλυσης εγκρίνει την έκθεση σκοπιμότητας σε συνεργασία με τον προμηθευτή (παραδοχές, περιορισμοί συστήματος, εκτίμηση κόστους λειτουργίας, εναλλακτικές λύσεις, απόδοση συστήματος, κ.λπ.).
- Κατά τη φάση της σχεδίασης, εγκρίνει τις τεχνικές προδιαγραφές (δομή συστήματος, επιλογή εξοπλισμού, διαδικασίες ελέγχου, αναφορές, περιγραφή αρχείων και βάσεων δεδομένων κ.λπ.).
- Κατά τη φάση της υλοποίησης, παρακολουθεί την ομαλή υλοποίηση των προδιαγραφών και συμμετέχει στην εγκατάσταση του λογισμικού και στο τεστ λειτουργίας του λογισμικού.

2.5. Νέες εφαρμογές / Αναβαθμίσεις λογισμικών

Πριν τον σχεδιασμό οποιασδήποτε νέας εφαρμογής ή την αναβάθμιση κάποιας υπάρχουσας, το Τμήμα Μηχανογράφησης ενημερώνεται από το εκάστοτε αρμόδιο Τμήμα και δίνει την τελική έγκριση.

Στην περίπτωση που, για την ικανοποίηση των αιτημάτων των Τμημάτων, απαιτείται η λήψη μηχανογραφικών υπηρεσιών, λογισμικού ή μηχανογραφικού εξοπλισμού από εξωτερικούς συνεργάτες τότε:

- Πραγματοποιείται η έγκριση της δαπάνης από το Δ.Σ. με σχετική εισήγηση από τον Διευθυντή του Ταμείου, και η επιλογή των εξωτερικών συνεργατών με βάση τη διαδικασία αγορών – πληροφορικής (αίτηση αγοράς, λήψη προσφορών, αξιολόγηση και έγκριση προμηθευτή, κ.λπ.).

- Όλα τα νέα μηχανογραφικά συστήματα ελέγχονται για να διασφαλιστεί η παροχή ακριβούς και έγκαιρης πληροφόρησης στη Διοίκηση του Ταμείου.

Στην περίπτωση που η μηχανογραφική εφαρμογή πρόκειται να καλυφθεί από το Ταμείο τότε:

- Καταρτίζεται πρόγραμμα ανάπτυξης και εγκατάστασης της εφαρμογής το οποίο φέρει και την έγκριση της Διοίκησης.
- Ορίζεται ο υπεύθυνος έργου ο οποίος αναλαμβάνει να κατευθύνει και να ελέγχει την πορεία ανάπτυξης και εφαρμογής του έργου.
- Κατανέμονται αντίστοιχα οι πόροι του Τμήματος και ορίζεται η ομάδα έργου.
- Διενεργείται έλεγχος λειτουργίας, κατά την ολοκλήρωση και πριν την παράδοση του έργου, έτσι ώστε να εντοπιστούν πιθανά προβλήματα και αδυναμίες και να επιλυθούν πριν η εφαρμογή τεθεί σε πλήρη λειτουργία.

Σε όλες τις περιπτώσεις παρέχεται κατάλληλη εκπαίδευση στο προσωπικό που χειρίζεται την εκάστοτε μηχανογραφική εφαρμογή, έτσι ώστε να ανταπεξέλθει στις ανάγκες χειρισμού της.

2.6. Ασφάλεια στο Περιβάλλον Ανάπτυξης και Υποστήριξης

Δεδομένα και συστήματα παραγωγής δεν χρησιμοποιούνται από το προσωπικό ανάπτυξης κατά την διαδικασία ανάπτυξης, ελέγχων και συντήρησης των εφαρμογών. Ο προσωρινός κώδικας (temporal code) ο οποίος χρησιμοποιείται κατά την διάρκεια των ελέγχων και της ανάπτυξης του νέου συστήματος / εφαρμογής, θα πρέπει να φυλάσσεται ξεχωριστά από τις εφαρμογές του περιβάλλοντος παραγωγής, οι οποίες είναι εγκατεστημένες στα συστήματα του Ταμείου. Όταν υφίστανται αλλαγές στα λειτουργικά συστήματα, τα συστήματα εφαρμογών ελέγχονται για να διασφαλιστεί ότι δεν υπάρχει κάποια αρνητική επίδραση στην ασφάλεια πληροφοριών, συμπεριλαμβανομένης της επανεξέτασης των μέτρων ασφάλειας των εφαρμογών και της ακεραιότητας των πληροφοριών τους, ώστε να διασφαλιστεί ότι δεν έχουν εκτεθεί σε κάποιο κίνδυνο από τις αλλαγές του λειτουργικού συστήματος.

Τα συστήματα ελέγχου και ανάπτυξης είναι καταλλήλως απομονωμένα από ενεργά (παραγωγικά) κρίσιμα συστήματα. Συγκεκριμένα:

- Στο προγραμματιστικό περιβάλλον (test environment) μόνο το εξουσιοδοτημένο προσωπικό έχει την δυνατότητα αλλαγών και τροποποιήσεων των προγραμμάτων.
- Τα στελέχη του προσωπικού ανάπτυξης (προγραμματιστές) δεν έχουν δικαίωμα αλλαγών κατά την διάρκεια της διαδικασίας προγραμματισμού. Με το πέρασμα της διαδικασίας στο περιβάλλον παραγωγής, ο κώδικας (code) κλειδώνεται και δεν μπορεί να τροποποιηθεί εκτός και αν επιστρέψει η διαδικασία στο στάδιο προγραμματισμού μέσω της διαδικασίας αλλαγών.
- Το προσωπικό ανάπτυξης δεν έχει πρόσβαση εγγραφής ή ενημέρωσης (write & update) στο περιβάλλον παραγωγής. Αντιθέτως, το προσωπικό διαχείρισης αλλαγών έχει το δικαίωμα μεταφοράς αρχείων στο περιβάλλον παραγωγής.

- Οι μεταγλωττιστές (compilers) δεν είναι εγκατεστημένοι στο περιβάλλον παραγωγής.

2.7. Διαχείριση πρόσβασης

Το Ταμείο ακολουθεί συγκεκριμένες οδηγίες που περιλαμβάνουν τις ακόλουθες απαιτήσεις/διαδικασίες:

- Ο Υπεύθυνος του Τμήματος Μηχανογράφησης διατηρεί μία ενημερωμένη λίστα εγκεκριμένων και εξουσιοδοτημένων χρηστών και των αντίστοιχων δικαιωμάτων πρόσβασής τους.
- Ο Υπεύθυνος του Τμήματος Μηχανογράφησης επεξεργάζεται όλα τα αιτήματα για πρόσβαση.
- Ο Υπεύθυνος του Τμήματος Μηχανογράφησης παράγει κωδικούς πρόσβασης για νέους χρήστες και, όταν κρίνεται απαραίτητο για τους υφιστάμενους χρήστες, και παρέχει τους κωδικούς με ασφαλή τρόπο. Εάν ένας υφιστάμενος χρήστης αντιμετωπίζει δυσκολία κατά την προσπέλασή του στο σύστημα, το Τμήμα Μηχανογράφησης πραγματοποιεί εκ νέου ρύθμιση και επιτρέπει στον χρήστη να δημιουργήσει ένα δικό του κωδικό πρόσβασης, εφόσον πρώτα έχει αναγνωριστεί η φυσική του ταυτότητα επιτυχώς. Η αναγνώριση απαιτείται όταν ο χρήστης λαμβάνει πληροφορίες για τον κωδικό πρόσβασης.
- Σε περίπτωση έκτακτης ανάγκης η πρόσβαση σε ευαίσθητες πληροφορίες πραγματοποιείται σύμφωνα με τις σχετικές εσωτερικές διαδικασίες.
- Τα συστήματα και οι εφαρμογές ορίζουν σαφώς τις ανάγκες του κάθε χρήστη ή ομάδας για τη πρόσβαση σε συστήματα, εφαρμογές και δεδομένα.
- Όλα τα προσωρινά στοιχεία αυθεντικοποίησης (default authentication data) τα οποία παρέχονται από τους Προμηθευτές νέου πληροφοριακού εξοπλισμού, τροποποιούνται πριν τα νέα συστήματα ενσωματωθούν στο περιβάλλον παραγωγής.

Κατά την διαδικασία προσδιορισμού των δικαιωμάτων πρόσβασης υπαλλήλου, ο Διευθυντής ενημερώνει γραπτώς το Τμήμα Μηχανογράφησης σχετικά με την πρόσληψη, αποχώρηση ή μεταφορά υπαλλήλου σε νέο Τμήμα. Στην περίπτωση πρόσληψης υπαλλήλου, Διευθυντής συμπληρώνει σχετικό έντυπο Προσβάσεων και το προωθεί στο Τμήμα Μηχανογράφησης προκειμένου να διενεργηθεί η υλοποίηση των δικαιωμάτων πρόσβασης. Ο Υπεύθυνος του Τμήματος Μηχανογράφησης δημιουργεί τους απαραίτητους λογαριασμούς και κωδικούς χρήστη σύμφωνα με την περιγραφή της αίτησης και ενημερώνει τον χρήστη αναλόγως.

Οι κωδικοί πρόσβασης αποτελούν την «πρώτη γραμμή» προστασίας για τους πληροφοριακούς πόρους του Ταμείου, εφόσον επιτρέπουν την πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες και απαγορεύουν την πρόσβαση σε μη εξουσιοδοτημένους ή κακόβουλους χρήστες.

Κάθε χρήστης του Πληροφοριακού Συστήματος του Ταμείου έχει έναν Λογαριασμό Χρήστη (User -ID)και ένα κωδικό πρόσβασης. Ο κάθε Λογαριασμός Χρήστη είναι μοναδικός και αυστηρά προσωπικός για κάθε χρήστη, όπως επίσης και κάθε κωδικός πρόσβασης αντιστοιχεί σε ένα και μόνο Λογαριασμό Χρήστη.

Το επίπεδο πρόσβασης του κάθε χρήστη καθορίζεται από τις αρμοδιότητες και τα καθήκοντά του, σύμφωνα με την αρχή του διαχωρισμού των αρμοδιοτήτων.

Κάθε αλλαγή στο επίπεδο πρόσβασης ή εξουσιοδότησης του χρήστη στο σύστημα εγκρίνεται κατάλληλα από τον Υπεύθυνο του Τμήματος Μηχανογράφησης.

Το επίπεδο πρόσβασης των χρηστών στο σύστημα επιθεωρείται περιοδικά, έτσι ώστε να εντοπίζονται τυχόν προσβάσεις από χρήστες σε αρχεία που δεν εντάσσονται στα πλαίσια των αρμοδιοτήτων και των καθηκόντων τους.

Ο προσωπικός Λογαριασμός Χρήστη:

- Είναι μοναδικός για κάθε χρήστη, ώστε να διασφαλίζεται η προσωπική του ευθύνη για τη χρήση του.
- Διαγράφεται όταν οι υπάλληλοι αποχωρούν από το Ταμείο.
- Περιορίζει την πρόσβαση του χρήστη σε συγκεκριμένες εντολές των προγραμμάτων.

Απαγορεύεται η ταυτόχρονη σύνδεση σε περισσότερες από μία θέσεις εργασίας με τον ίδιο Λογαριασμό Χρήστη.

Οι κωδικοί πρόσβασης,

- Έχουν προκαθορισμένο ελάχιστο και μέγιστο πλήθος χαρακτήρων και συγκεκριμένη πολυπλοκότητα. Αυτό σημαίνει ότι ο χρήστης δεν μπορεί να χρησιμοποιεί απλές φράσεις ή αριθμούς για την πρόσβαση στο δίκτυο. Συγκεκριμένα η δομή του κάθε κωδικού περιλαμβάνει την ύπαρξη μικρών και κεφαλαίων χαρακτήρων, αριθμούς και σύμβολα.
- Ο κωδικός κάθε χρήστη αλλάζει με περιοδικότητα τριμήνου.
- Ο κάθε χρήστης δε μπορεί να χρησιμοποιήσει εκ νέου τους τελευταίους 12 κωδικούς.
- Δεν εμφανίζονται στην οθόνη κατά την πληκτρολόγησή τους.
- Υπάρχει πάντα ενεργοποιημένη διαδικασία για τον εντοπισμό των προσπαθειών εισόδου στο σύστημα με λάθος κωδικό. Συγκεκριμένα, μετά τις τρεις (3) λανθασμένες προσπάθειες πρόσβασης, το σύστημα κλειδώνει αυτόματα για 15’.
- Δεν πρέπει να υπάρχει ταυτόχρονη σύνδεση σε περισσότερες από μία θέσεις εργασίας με τον ίδιο κωδικό. Είναι αυστηρά προσωπική για κάθε χρήστη και δεν πρέπει να ανακοινώνεται σε τρίτους.
- Σε συνεργασία με την Διεύθυνση λαμβάνεται ειδική μέριμνα για την απενεργοποίηση των λογαριασμών και των κωδικών πρόσβασης των εργαζομένων που αποχωρούν από το Ταμείο.
- Η αυστηρή τήρηση των κανόνων δημιουργίας και συντήρησης των κωδικών πρόσβασης είναι αποκλειστική ευθύνη του Υπευθύνου του Τμήματος Μηχανογράφησης.
- Η ακριβής διαδικασία πρόσβασης από remote users στο σύστημα διασφαλίζεται με την περιοδική αλλαγή των κωδικοί πρόσβασης από το Τμήμα Μηχανογράφησης.

2.8. Έλεγχος πρόσβασης

Όλα τα μέτρα ελέγχου πρόσβασης που έχουν αναπτυχθεί από το Ταμείο ενσωματώνουν συγκεκριμένες λειτουργίες που είναι πλήρως καταγεγραμμένες και ελεγχόμενες. Επιπλέον, τα εν λόγω μέτρα διαμορφώνονται καταλλήλως ώστε να παρέχουν τις εξής λειτουργίες:

- Υποστήριξη των αρχών ασφάλειας «ελάχιστων προνομίων» (least privileged) και «αναγκαίας γνώσης» (need-to-know).
- Οι δικαιοδοτήσεις πρόσβασης πρέπει να είναι ανιχνεύσιμες βάσει της ταυτότητας του εκάστοτε χρήστη. Δεν πρέπει να παρέχεται προ-εγκατεστημένη (default) πρόσβαση σε οποιοδήποτε σύστημα.
- Οι ταυτότητες χρηστών για τους υπαλλήλους πρέπει να απενεργοποιούνται μετά από εξήντα (60) ημέρες αδράνειας και να διαγράφονται μετά από ενενήντα (90) ημέρες αδράνειας, εκτός εάν παραταθούν μετά από την αποκλειστική έγκριση της Διοίκησης.
- Η αλλαγή της κατάστασης του υπαλλήλου (μέσα στο Ταμείο) συνεπάγεται αντίστοιχη αλλαγή των δικαιωμάτων πρόσβασης, το πολύ εντός είκοσι τεσσάρων (24) ωρών.
- Οι συνεδρίες (sessions) χρηστών περιορίζονται στον μέγιστο χρόνο των είκοσι (20) λεπτών, χρησιμοποιώντας είτε διακοπή συνεδρίας (session time out) είτε οθόνη προστατευόμενη από κωδικό πρόσβασης. Στο εν λόγω μέτρο δεν περιλαμβάνονται εργασίες/εφαρμογές που λειτουργούν σε background επίπεδο του συστήματος, χωρίς την ύπαρξη συνεδρίας και οι προστασίες οθόνης προσωπικών υπολογιστών.

2.9. Αυθεντικοποίηση των χρηστών

Σύμφωνα με την Διαδικασία του Ταμείου, απαιτείται η αυθεντικοποίηση των χρηστών για την πρόσβασή τους στα Πληροφοριακά του Συστήματα. Το Ταμείο εφαρμόζει συγκεκριμένες μεθόδους αυθεντικοποίησης (Λογαριασμός Χρήστη, κωδικός πρόσβασης κ.λπ.). Η μέθοδος αυθεντικοποίησης εξαρτάται από τον τύπο του Πληροφοριακού Συστήματος για τον οποίο ο χρήστης αιτείται πρόσβασης και το βαθμό ευαισθησίας των πληροφοριών που διαχειρίζεται το συγκεκριμένο Πληροφοριακό Σύστημα του Ταμείου.

Οι συνηθέστερες πρακτικές που ακολουθεί το Ταμείο για θέματα αυθεντικοποίησης είναι:

- Χρήση πολλαπλών ελέγχων εξουσιοδότησης.
- Περιορισμός των δικαιωμάτων του χρήστη.
- Χρήση επιπέδων εξουσιοδότησης.

Ανεξάρτητα από τη μέθοδο αυθεντικοποίησης, ακολουθούνται οι εξής κανόνες για τη διασφάλιση της κατάλληλης αυθεντικοποίησης των χρηστών του Ταμείου:

- Όλα τα πληροφοριακά συστήματα του Ταμείου εφαρμόζουν μηχανισμούς αυθεντικοποίησης εγκεκριμένους από τον Υπεύθυνο του Τμήματος Μηχανογράφησης.
- Η χρήση κοινόχρηστων και γενικών λογαριασμών (default accounts) πρόσβασης σε πληροφοριακά συστήματα απαγορεύεται. Στην περίπτωση απώλειας ή υποκλοπής στοιχείων αυθεντικοποίησης (δηλαδή κωδικοί πρόσβασης, «έξυπνες κάρτες», όνομα χρήστη, PIN κ.λπ.), ο χρήστης ενημερώνει τον Υπεύθυνο του Τμήματος Μηχανογράφησης προκειμένου να λάβει τα κατάλληλα μέτρα.

- Η πρόσβαση σε αρχεία ασφάλειας, αρχεία διαχείρισης/διαμόρφωσης συστημάτων, η δημιουργία κοινόχρηστων δίσκων ή άλλων προστατευόμενων φακέλων πραγματοποιείται μόνο από τον Υπεύθυνο του Τμήματος Μηχανογράφησης, ο οποίος χρειάζεται την εν λόγω πρόσβαση προκειμένου να ασκήσει τα καθήκοντά του. Χρήστες με πρόσβαση Προγραμματιστή, διαχειριστή συστήματος ή δικτύου οι οποίοι διαθέτουν προνομιούχα δικαιώματα πρόσβασης, απαγορεύεται να χρησιμοποιούν τα εν λόγω δικαιώματα για πρόσβαση σε προσωπικά αρχεία (π.χ. e-mails, αναφορές κ.τ.λ.) άλλων χρηστών, και γενικότερα για μη εξουσιοδοτημένες ενέργειες.
- Όλες οι τεχνολογικές πλατφόρμες πρέπει να αυθεντικοποιούν (επαληθεύουν) την ταυτότητα των χρηστών (ή άλλων απομακρυσμένων συστημάτων) πριν την έναρξη οποιασδήποτε συνεδρίας, σύνδεσης ή συναλλαγής.

3. Διαδικασία πρόσβασης Εξωτερικών Συνεργατών

3.1. Έγκριση Αίτησης Εξωτερικού Συνεργάτη

Οι εξωτερικοί συνεργάτες που επιθυμούν πρόσβαση και διασύνδεση με τα Πληροφοριακά και Δικτυακά Συστήματα του Ταμείου, συμπληρώνουν και υπογράφουν μία σχετική αίτηση διασύνδεσης την οποία καταθέτουν στο Τμήμα Μηχανογράφησης. Το Τμήμα Μηχανογράφησης, προωθεί το αίτημα στον Διευθυντή του Ταμείου όπου αποφασίζει την τελική έγκριση ή απόρριψή του.

Ο Υπεύθυνος του Τμήματος Μηχανογράφησης του Ταμείου διατηρεί αρχείο διασυνδέσεων και προσβάσεων στα συστήματα και καταγράφει όλο το σχετικό ιστορικό.

4. Ασφάλεια Μηχανογραφικών Συστημάτων

4.1. Αρχιτεκτονική Δικτύου

Το Ταμείο εδραιώνει την αρχιτεκτονική ασφάλειας του δικτύου του, προσδιορίζοντας την ασφάλεια υποδομής, τη συνδεσιμότητα, και τις ενέργειες συντήρησής της. Μία άρτια σχεδιασμένη, και λειτουργική αρχιτεκτονική δικτύου είναι απαραίτητη για να προστατεύσει αποτελεσματικά τις πληροφορίες που μεταφέρονται στα δίκτυα υπολογιστών του Ταμείου.

4.2. Υποδομή Δικτύου

4.2.1. Τείχος προστασίας (Firewall)

Η τεχνολογία των τειχών προστασίας εφαρμόζεται στη περίμετρο του δικτύου του Ταμείου για να προστατεύσει τους ευαίσθητους εσωτερικούς πληροφοριακούς πόρους από μη εξουσιοδοτημένη πρόσβαση. Τα τείχη προστασίας ενσωματώνουν τα ακόλουθα χαρακτηριστικά:

- Η Εξωτερική και η Εσωτερική (εισερχόμενη και εξερχόμενη) κίνηση δρομολογείται μέσω των τειχών προστασίας.
- Προκαθορισμένη Αρχή Απαγόρευσης (Default Deny Principle). Μόνο η δικτυακή κίνηση η οποία ρητώς επιτρέπεται από την πολιτική, επιτρέπεται και από το τείχος προστασίας. Κάθε άλλου είδους δικτυακή κίνηση εμποδίζεται από τον προκαθορισμένο κανόνα απαγόρευσης (default deny rule) του τείχους προστασίας.

Όλες οι παρεισφρήσεις καταγράφονται σε σχετικά αρχεία (log file) τα οποία συγκεντρώνονται σε μία εφαρμογή κεντρικής διαχείρισης, η οποία ελέγχεται από τον Υπεύθυνο του Τμήματος Μηχανογράφησης. Τα εν λόγω αρχεία καταγράφουν την ημερομηνία και την ώρα της τελευταίας επιτυχούς εισόδου καθώς και τον αριθμό των ανεπιτυχών προσπαθειών εισόδου στο σύστημα μετά την τελευταία επιτυχή είσοδο.

Η παραμετροποίηση του τείχους προστασίας καταγράφεται και είναι μέρος της διαδικασίας διαχείρισης αλλαγών του Ταμείου.

4.2.2. Φίλτρα περιεχομένου υπηρεσιών e-mail & Web

Φίλτρα Περιεχομένου τοποθετούνται στο δίκτυο του Ταμείου για να ελέγχουν την ηλεκτρονική αλληλογραφία και τις υπηρεσίες Web που παρέχονται στους εργαζόμενους του Ταμείου. Συγκεκριμένα:

- Λογισμικό φιλτραρίσματος του Web περιεχομένου εφαρμόζεται στον Web Proxy ή στους δρομολογητές (routers) του Internet για να αποτρέψουν τους χρήστες του Ταμείου από το να έχουν πρόσβαση σε ακατάλληλο περιεχόμενο του διαδικτύου.
- Επιπρόσθετα, το δίκτυο του Ταμείου ενσωματώνει λογισμικό φιλτραρίσματος περιεχομένου της ηλεκτρονικής αλληλογραφίας που εξετάζει την πληροφορία που περιέχεται στην επικεφαλίδα του μηνύματος (θέμα) για να απορρίψει ή να επιτρέψει ένα μήνυμα βάσει των διαδικασιών του Ταμείου.

Είναι σημαντικό να αναφερθεί ότι πριν την εγκατάσταση του λογισμικού φιλτραρίσματος περιεχομένου, η Νομική Υπηρεσία του Ταμείου είναι υπεύθυνη να εξετάσει τους σχετικούς νόμους και κανονισμούς οι οποίοι ενδέχεται να απαγορεύουν τη χρήση τέτοιου λογισμικού.

Το Τμήμα Μηχανογράφησης του Ταμείου είναι υπεύθυνο για την ορθή εγκατάσταση και παραμετροποίηση των φίλτρων περιεχομένου ηλεκτρονικής αλληλογραφίας και web.

4.2.3. Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System (IDS))

Σύστημα Ανίχνευσης Εισβολών εγκαθίστανται στο δίκτυο του Ταμείου για την αποτελεσματική ανίχνευση και ανταπόκριση σε επιθέσεις από διάφορους κακόβουλους χρήστες του Internet και από, ακούσια ή σκόπιμη, κακή χρήση των δικτυακών πόρων του Ταμείου από τους εσωτερικούς του χρήστες. Αισθητήρες ανίχνευσης εισβολών εγκαθίστανται στρατηγικά στις αποστρατικοποιημένες ζώνες (Demilitarized Zones ((DMZ)) του Ταμείου, σε συγκεκριμένες συσκευές ή στη περίμετρο των δικτύων. Η τοποθέτηση των αισθητήρων εξαρτάται από το τύπο του Συστήματος Ανίχνευσης εισβολών:

- Δικτυακοί αισθητήρες (network-based sensors) συνδέονται στον δικτυακό εξοπλισμό του Ταμείου (switches, routers και hubs) για να εξετάζουν την κίνηση του δικτύου.
- Αισθητήρες εφαρμογών (application-based sensors) τοποθετούνται στο μπροστινό τμήμα μίας ομάδας εξυπηρετητών (servers) για να παρακολουθούν και να αναλύουν την επικοινωνία μεταξύ των χρηστών (clients) και του εξυπηρετητή της εφαρμογής (application server).
- Αισθητήρες πρωτοκόλλων (protocol-based sensors) τοποθετούνται στον εξυπηρετητή για να αναλύουν / εξετάζουν το πρωτόκολλο επικοινωνίας μεταξύ του εξυπηρετητή και της συνδεδεμένης συσκευής.
- Αισθητήρες σταθμών εργασίας (host-based sensors) παρακολουθούν και αναλύουν την συμπεριφορά ενός συγκεκριμένου σταθμού που είναι συνδεδεμένος στο δίκτυο εξετάζοντας τις κλήσεις του συστήματος και των εφαρμογών του, την τροποποίηση των αρχείων του κ.τ.λ.

Το Τμήμα Μηχανογράφησης του Ταμείου είναι υπεύθυνο για την εγκατάσταση και λειτουργία όλων των συστημάτων και αισθητήρων ανίχνευσης / αποτροπής εισβολών. Ο Υπεύθυνος του Τμήματος Μηχανογράφησης έχει την επίβλεψη της λειτουργίας του Συστήματος Ανίχνευσης Εισβολής. Η παραμετροποίηση του συστήματος ανίχνευσης εισβολών απαιτείται να είναι καταγεγραμμένη και να υπόκειται στην διαδικασία διαχείρισης αλλαγών του Ταμείου.

4.2.4. Δρομολογητές (Routers)

Οι δρομολογητές του Ταμείου που χρησιμοποιούνται για την δρομολόγηση της εισερχόμενης και εξερχόμενης κίνησης των χρηστών του, παραμετροποιούνται σύμφωνα με τις οδηγίες του Ταμείου. Οι δρομολογητές που ενσωματώνουν firewalls, έλεγχο πρόσβασης και άλλες λειτουργίες ασφάλειας χρησιμοποιούνται στρατηγικά για να παρέχουν τις εν λόγω υπηρεσίες μαζί με τη δρομολόγηση δεδομένων. Ο Υπεύθυνος του Τμήματος Μηχανογράφησης έχει την ευθύνη να αποφασίσει που θα εγκατασταθούν οι δρομολογητές με τις λειτουργίες ασφάλειας και την ευθύνη για την εγκατάσταση και παραμετροποίηση τους.

4.2.5. Δικτυακός Εξοπλισμός Υποδομής

Ο δικτυακός εξοπλισμός υποδομής του Ταμείου (π.χ. καλώδια ethernet, οπτικές ίνες, ασύρματος εξοπλισμός, συσκευές διασύνδεσης δικτύων) που χρησιμοποιείται για να συνδέει τους διανεμημένους πόρους των δικτύων, προστατεύεται από το Τμήμα Μηχανογράφησης.

4.3. Πρόσβαση Δικτύου

4.3.1. Απομακρυσμένη πρόσβαση (Remote access)

Απομακρυσμένη Πρόσβαση στους δικτυακούς πόρους, από τα στελέχη του Ταμείου που αιτούνται αυτόν τον τύπο υπηρεσίας, δίδεται μέσω της διαδικασίας Απομακρυσμένης Πρόσβασης μέσω VPN. Για να εδραιώσει την ασφάλεια και τη συνεχή σταθερότητα στις απομακρυσμένες συνδέσεις, το Ταμείο, διατηρεί Σημεία Απομακρυσμένης Πρόσβασης (remote access points) παρέχοντας πρόσβαση στο απομακρυσμένο, εξουσιοδοτημένο προσωπικό της. Το Σημείο Απομακρυσμένης Πρόσβασης ελέγχει την πρόσβαση των χρηστών μέσω Μηχανισμών Αυθεντικοποίησης που ενσωματώνουν λειτουργίες αυθεντικοποίησης (authentication), εξουσιοδότησης (authorization) και απόδοσης ευθυνών (accountability).

Ο εργαζόμενος ή εξωτερικός συνεργάτης που επιθυμεί να έχει απομακρυσμένη πρόσβαση, υποβάλει σχετική αίτηση στο Διευθυντή του Ταμείου, η οποία και εγκρίνει την παροχή της πρόσβασης. Ο Υπεύθυνος του Τμήματος Μηχανογράφησης έχει την ευθύνη να παρέχει το δικαίωμα απομακρυσμένης πρόσβασης στους εργαζόμενους, κατόπιν έγκρισης της Διεύθυνσης εφόσον συγκεκριμένα επιχειρησιακά θέματα απαιτείται να διευθετηθούν μέσω αυτής.

4.3.2. Έλεγχος πρόσβασης Ασύρματου Τοπικού Δικτύου (WLAN)

Τα σημεία ασύρματης πρόσβασης του Ταμείου συνδέονται στο ενσύρματο δίκτυο με την κατάλληλη παραμετροποίηση. Ο Υπεύθυνος του Τμήματος Μηχανογράφησης έχει την ευθύνη για την διαχείριση της εγκατάστασης των σημείων ασύρματης πρόσβασης ώστε να διασφαλίσει ότι ακολουθούνται οι βέλτιστες πρακτικές ασφάλειας σχετικά με την ασύρματη τεχνολογία. Προσωπικό ή επισκέπτες που επιθυμούν να συνδεθούν στο ασύρματο τοπικό δίκτυο κάνουν αίτηση για σύνδεση προφορικά στον Υπεύθυνο του Τμήματος Μηχανογράφησης.

Το Ταμείο έχει υιοθετήσει τους παρακάτω ελεγκτικούς μηχανισμούς σχετικά με την πρόσβαση στο ασύρματο τοπικό δίκτυο:

- Κρυπτογράφηση δεδομένων, ώστε η πρόσβαση στις πληροφορίες να επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες
- Έλεγχος ταυτότητας χρηστών, ο οποίος αναγνωρίζει τους υπολογιστές που επιχειρούν να αποκτήσουν πρόσβαση στο δίκτυο.
- Πρόσβαση υψηλής ασφαλείας για επισκέπτες και εξωτερικούς χρήστες.
- Καταχώρηση – ονοματοδοσία των χρηστών του ασύρματου δικτύου.

4.4. Προστασία από κακόβουλο λογισμικό

Η επιτυχία ενός προγράμματος ασφάλειας από κακόβουλο λογισμικό έγκειται στην αυστηρή εφαρμογή διαδικασιών ασφάλειας σε συνδυασμό με την ενημέρωση και εκπαίδευση του υπεύθυνου προσωπικού του Ταμείου ώστε να διασφαλιστεί η μέγιστη κάλυψη σε σχέση με τη σάρωση (scan) των σταθμών εργασίας και των διακομιστών (servers) για την εύρεση πιθανού κακόβουλου λογισμικού.

Το λογισμικό / πρόγραμμα προστασίας που χρησιμοποιείται για τη προστασία των πληροφοριακών συστημάτων του Ταμείου έχει τα ακόλουθα χαρακτηριστικά:

- Το πρόγραμμα ασφάλειας από κακόβουλο λογισμικό είναι εγκατεστημένο σε όλους τους σταθμούς εργασίας, φορητούς υπολογιστές και διακομιστές.
- Οι δικτυακές πύλες (gateways) έχουν εγκατεστημένο το λογισμικό προστασίας από ιούς.
- Το Τμήμα Μηχανογράφησης διασφαλίζει ότι το πρόγραμμα προστασίας από κακόβουλο λογισμικό που είναι εγκατεστημένο στους σταθμούς εργασίας είναι σύμφωνο με την πολιτική, λειτουργεί και αναβαθμίζεται τακτικά όπως έχει καθοριστεί και δεν έχει τροποποιηθεί ή αφαιρεθεί..
- Οι χρήστες δεν απενεργοποιούν ή δεν τροποποιούν το εγκατεστημένο λογισμικό προστασίας στους υπολογιστές τους.
- Το Ταμείο έχει εγκρίνει και ελέγχει διαρκώς τις οδηγίες παραμετροποίησης του προγράμματος προστασίας από κακόβουλο λογισμικό οι οποίες ακολουθούνται κατά την εγκατάσταση.

Προκειμένου το Τμήμα Μηχανογράφησης να ελέγχει την εξουσιοδοτημένη πρόσβαση στο δίκτυο δεδομένων του Ταμείου, έχει εγκατασταθεί ένα σύνολο από εξειδικευμένα προϊόντα που εξυπηρετούν το σκοπό αυτό. Υπάρχει εγκατεστημένο λογισμικό το οποίο ελέγχει την πρόσβαση στο διαδίκτυο, υπάρχει λογισμικό το οποίο παρακολουθεί συνεχώς την κίνηση του δικτύου, καθώς επίσης και λογισμικό ενάντια σε κακόβουλο λογισμικό (antivirus).

Πιο αναλυτικά, υπάρχει συγκεκριμένο λογισμικό το οποίο είναι υπεύθυνο για την συνεχή παρακολούθηση της κίνησης από και προς το διαδίκτυο και της κίνησης στο εσωτερικό δίκτυο του Ταμείου και επίσης είναι επιφορτισμένο με κανόνες οι οποίοι υπαγορεύουν τον τρόπο με τον οποίο ένας υπολογιστής συνδέεται στο διαδίκτυο. Τέλος, ελέγχει και τα αρχεία τα οποία ο χρήστης αποθηκεύει στον υπολογιστή του (download) από το διαδίκτυο.

Επίσης, σε κάθε υπολογιστή του Ταμείου, είναι εγκατεστημένο σχετικό πρόγραμμα το οποίο παρακολουθεί κακόβουλα λογισμικά (computer virus, trojan). Το πρόγραμμα αυτό , μέσω διαδικτύου, διενεργεί έλεγχο ημερησίως, έτσι ώστε να μπορεί να παρακολουθεί τυχόν νέων απειλών που δημιουργούνται στο διαδίκτυο και να είναι δυνατή η ανίχνευση και των πιο τεχνολογικά εξελιγμένων ιών που είναι πιθανό να εισέλθουν στο σύστημα. Στα πλαίσια προφύλαξης των συστημάτων από ιούς, όλα τα μέσα αποθήκευσης πληροφοριών (usb sticksCD roms, κ.λπ.), τα οποία προέρχονται από εξωτερικές πηγές, πριν από τη χρήση τους ελέγχονται αυτόματα για την ύπαρξη ιών. Σε περίπτωση που ανιχνευθεί ιός πρέπει να «καθαρίζονται» ή να απαγορεύεται η χρήση τους. Επιπλέον, η πρόσβαση στο διαδίκτυο είναι ελεγχόμενη. Ο χρήστης δεν μπορεί να δει απαγορευμένες σελίδες (π.χ. ακατάλληλο περιεχόμενο, σελίδες στοιχημάτων, σελίδες μέσων κοινωνικής δικτύωσης) ενώ ταυτόχρονα η πρόσβαση στο διαδίκτυο ελέγχεται, για πιθανές «επιδρομές» από hackers και κακόβουλους χρήστες.

5. Φυσική προστασία πληροφοριακού εξοπλισμού

Όλο το προσωπικό είναι υπεύθυνο για την προστασία του πληροφοριακού εξοπλισμού που υπάρχει στο εργασιακό τους περιβάλλον. Οι παρακάτω κανόνες φυσικής ασφάλειας εφαρμόζονται σε όλα τα γραφεία, δωμάτια, χώρους και λοιπές εγκαταστάσεις του Ταμείου:

- Δεν πρέπει να υπάρχουν φαγητά και ποτά κοντά στα πληροφοριακά συστήματα.
- Όλοι οι εργαζόμενοι πρέπει να αποσυνδέονται από τα πληροφοριακά συστήματα όταν αποχωρούν από την περιοχή εργασίας τους για οποιονδήποτε λόγο.
- Οι εργαζόμενοι πρέπει να προστατεύουν τα δεδομένα που περιέχονται σε εκτυπωμένα έγγραφα και άλλα μέσα, προστατεύοντας ευαίσθητα δεδομένα σε κλειδωμένα ντουλάπια/φωριαμούς όταν δεν χρησιμοποιούνται είτε καταστρέφοντάς τα με ειδικά μηχανήματα (καταστροφείς) ή μέσω άλλων εγκεκριμένων μεθόδων καταστροφής.
- Η χρήση προστασίας οθόνης (Screen saver) η οποία ενεργοποιείται έπειτα από 30 (ή λιγότερα) λεπτά αδράνειας και η υποχρεωτική επανασύνδεση με κωδικό πρόσβασης, προτείνεται όπου κάτι τέτοιο μπορεί να εφαρμοσθεί. Οι χρήστες πρέπει να προστατεύουν τους κωδικούς προστασίας οθόνης των υπολογιστών τους και να μην τους γνωστοποιούν.
- Οι Υπεύθυνοι Τμημάτων είναι αρμόδιοι να κρατούν ενήμερο το προσωπικό για τις κατάλληλες διαδικασίες προστασίας από πυρκαγιά, , προστασία εξοπλισμού και πληροφοριών και αναφορά κλοπής πληροφοριακών αγαθών.
- Οι Υπεύθυνοι Τμημάτων είναι αρμόδιοι να διασφαλίζουν ότι όλα τα απαραίτητα μέτρα προστασίας των σταθμών εργασίας και του υπολοίπου περιφερειακού εξοπλισμού, μέσα στους χώρους ευθύνης τους, έχουν ληφθεί για την πρόληψη κλοπής, κατάχρησης ή μη- εξουσιοδοτημένης χρήσης.

Ο πληροφοριακός εξοπλισμός είναι ασφαλώς τοποθετημένος και προστατευμένος με σκοπό την ελαχιστοποίηση του κινδύνου καταστροφής ή απώλειας από περιβαλλοντικές καταστροφές, κλοπές, ατυχήματα ή κακόβουλες πράξεις:

- Πρόσβαση στο χώρο φύλαξης του κεντρικού μηχανογραφικού εξοπλισμού του Ταμείου καθώς και στα συστήματα του επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα. Για την πρόσβαση στο χώρο του κεντρικού μηχανογραφικού εξοπλισμού του Ταμείου απαιτείται κάρτα εισόδου.
- Η περιοχή εντός και γύρω από τον χώρο του κέντρου ηλεκτρονικών υπολογιστών διαθέτει πυροπροστασία , αντιπλημμυρική προστασία, καθώς και μέτρα ενάντια σε άλλους κινδύνους όπως διακοπές ρεύματος και συνθήκες ακραίων θερμοκρασιών.
- Οι εξυπηρετητές αρχείων που περιέχουν πληροφορίες του Ταμείου είναι εγκατεστημένοι σε ασφαλείς περιοχές ώστε να αποτραπεί κλοπή, καταστροφή ή μη εξουσιοδοτημένη πρόσβαση σε αυτούς. Μέτρα φυσικής πρόσβασης περιλαμβάνουν οποιονδήποτε συνδυασμό των μέτρων της προηγούμενης παραγράφου.
- Υπάρχουν διαδικασίες για την διασφάλιση επείγουσας πρόσβασης.
- Υπάρχουν διαδικασίες που διασφαλίζουν τον ορθό έλεγχο του εξοπλισμού.

Οι ηλεκτρικές γεννήτριες συμμορφώνονται με τα πρότυπα που προτείνονται από τον κατασκευαστή. Επιπρόσθετα, ο κρίσιμος πληροφοριακός εξοπλισμός του Ταμείου προστατεύεται από διακοπές ηλεκτρικού ρεύματος, αυξομειώσεις ηλεκτρικής τάσης ή άλλων ηλεκτρικών ανωμαλιών.

Οι καλωδιώσεις ρεύματος και δεδομένων (τηλεπικοινωνιών) εγκαθίστανται με τέτοιο τρόπο ώστε να αποφεύγονται περιβαλλοντικοί κίνδυνοι, όπως επίσης και περιπτώσεις ατυχήματος ή κακόβουλων πράξεων. Εάν η καλωδίωση μεταφέρει υψηλού επιπέδου ευαίσθητες πληροφορίες σε μία μη ελεγχόμενη (δημόσιας πρόσβασης) περιοχή που δεν μπορεί να προστατευθεί φυσικά από υποκλοπές, τα δεδομένα προστατεύονται με την χρήση κρυπτογράφησης. Όλα τα καλώδια δεδομένων, ανεξαρτήτως της πληροφορίας που μεταφέρεται δια μέσου αυτών, είναι καλυμμένα ώστε να προστατεύονται και να ελαχιστοποιείται ενδεχόμενη ηλεκτρονική παγίδευση ή υποκλοπή των δεδομένων που μεταφέρουν.

5.1. Συντήρηση συστημάτων

Υπεύθυνος για τον εντοπισμό της ανάγκης συντήρησης των συστημάτων του Ταμείου είναι ο Υπεύθυνος του Τμήματος Μηχανογράφησης και ο αντίστοιχος χρήστης.

Με τον όρο συντήρηση, εννοούμε οποιαδήποτε αλλαγή στο υλικό, στο λογισμικό, διορθώσεις σφαλμάτων, αντιμετώπιση νέων απαιτήσεων ή βελτίωση της απόδοσης των συστημάτων.

Σε εβδομαδιαία βάση, ο Υπεύθυνος του Τμήματος Μηχανογράφησης, διενεργεί ελέγχους ως προς την επιτυχή λειτουργία των εφεδρικών συστημάτων (back up) και των αρχείων καταγραφής των συστημάτων, όπου αυτά είναι διαθέσιμα (log files) προκειμένου να ελεγχθεί η ορθή λειτουργία των συστημάτων. Επίσης, εκτελεί και οπτικούς ελέγχους σε όλα τα συστήματα ώστε να διασφαλίζεται και να επιβεβαιώνεται η ορθή λειτουργία τους.

Σε περίπτωση εντοπισμού προβλήματος πραγματοποιείται μια αρχική ανάλυσή και ανάλογα με τα χαρακτηριστικά του αποφασίζεται εάν αυτό δύναται να επιλυθεί εσωτερικά. Σε περίπτωση που η συντήρηση καλύπτεται από σχετική σύμβαση, ο Υπεύθυνος του Τμήματος Μηχανογράφησης επικοινωνεί με την αρμόδια εταιρεία προκειμένου να διενεργηθεί η προγραμματισμένη ή μη συντήρηση των συστημάτων της.

6. Άδειες χρήσης λογισμικών

Το Ταμείο υποστηρίζει σταθερά την αυστηρή τήρηση των όρων των Αδειών Χρήσης Λογισμικού. Για το λόγο αυτό οι χρήστες μεταχειρίζονται πάσης φύσης λογισμικό σύμφωνα με τους όρους της Άδειας Χρήσης του. Το Τμήμα Μηχανογράφησης είναι αρμόδιο για την εγκατάσταση κατάλληλα εξουσιοδοτημένων λογισμικών στους υπολογιστές του Ταμείου τα οποία συνοδεύονται από τις αντίστοιχες άδειες χρήσης.

Πιο αναλυτικά, απαγορεύεται κάθε είδους χρήση, εγκατάσταση, αντιγραφή λογισμικού που δεν είναι σύμφωνη με την Άδεια Χρήσης του. Επιπρόσθετα, το προσωπικό πρέπει να θεωρεί ότι κάθε λογισμικό υπόκειται σε δικαιώματα δημιουργού, εκτός αν υπάρχει συγκεκριμένη δήλωση που εκφράζει σαφώς το αντίθετο.

Επίσης, ανά τακτά χρονικά διαστήματα παρακολουθούνται από τον Υπεύθυνο του Τμήματος Μηχανογράφησης οι ανάγκες για ανανέωση των αδειών χρήσης μέσω αρχείου excel. Η διάρκεια της άδειας χρήσης αναφέρεται στη σύμβαση άδειας χρήσης λογισμικού με τον προμηθευτή.

7. Οδηγίες χρήσης λογισμικού και εφαρμογών

Το Ταμείο υποστηρίζει τη χρήση Λογισμικών και Εφαρμογών από κατάλληλα εγκεκριμένους και εξουσιοδοτημένους παρόχους. Για το λόγο αυτό τα νέα λογισμικά ή οι εφαρμογές που εγκαθίστανται στα πληροφοριακά συστήματα του Ταμείου, πέρα από τις Άδειες χρήσης τους, φέρουν και τα κατάλληλα εγχειρίδια οδηγιών χρήσης τους προς εξυπηρέτηση των χρηστών.

Για τις περιπτώσεις κατά τις οποίες τα λογισμικά ή οι εφαρμογές κατασκευάζονται από το Τμήμα Μηχανογράφησης του Ταμείου, ο Υπεύθυνος του Τμήματος είναι αρμόδιος για τη σύνταξη και κοινοποίηση στο προσωπικό του Ταμείου των εν λόγω εγχειριδίων.

8. Διαδικασία διαχείρισης προβλημάτων χρηστών

Ο σκοπός αυτής της διαδικασίας είναι να καθορίσει τον τρόπο με τον οποίο γνωστοποιούνται, αξιολογούνται και αντιμετωπίζονται σε καθημερινή βάση τα μηχανογραφικά προβλήματα που εμφανίζονται τόσο σε επίπεδο εξοπλισμού όσο και σε επίπεδο εφαρμογών.

Το Τμήμα Μηχανογράφησης, δέχεται από το σύνολο των Τμημάτων του Ταμείου, διάφορα αιτήματα που άπτονται μηχανογραφικής υποστήριξης μέσω ηλεκτρονικής φόρμας ή σχετικού γραπτού μηνύματος. Αυτά τα αιτήματα, αρχειοθετούνται σε καθημερινή βάση από τον Υπεύθυνο του Τμήματος Μηχανογράφησης, και στη συνέχεια ιεραρχούνται και αξιολογούνται. Η διαδικασία αξιολόγησης και ιεράρχησης πραγματοποιείται με γνώμονα την επίπτωση του προβλήματος στις επιχειρησιακές λειτουργίες και στόχο την όσο το δυνατόν πιο άμεση ανταπόκριση επίλυση του εκάστοτε προβλήματος.

Με τον τρόπο αυτό, επιτυγχάνεται η άμεση, σωστή και έγκαιρη αντιμετώπιση των προβλημάτων που ανακοινώνονται στο Τμήμα Μηχανογράφησης, και διασφαλίζεται η ομαλή λειτουργία του Ταμείου.

Συγκεκριμένα η ροή της διαδικασίας έχει ως εξής:

Ο Υπεύθυνος του Τμήματος Μηχανογράφησης, καταγράφει σε σχετική λίστα τα αιτήματα από τους χρήστες του Ταμείου. Κατόπιν, δίνει την σήμανση του προβλήματος (χαρακτηρισμός βάσει σημαντικότητας) και προχωράει στην επίλυσή του. Όταν το πρόβλημα αποκατασταθεί, ενημερώνεται και η σχετική λίστα που αναφέρθηκε παραπάνω και η επίλυση κοινοποιείται με απάντηση (απάντηση πάνω στην αρχική ηλεκτρονική φόρμα) στον αιτούντα επίλυσης του προβλήματος. Επίσης, ο Υπεύθυνος του Τμήματος Μηχανογράφησης, συντάσσει αναφορά στην οποία καταγράφει τις ενέργειες που εκτέλεσε και την οποία αποστέλλει στον Διευθυντή προς ενημέρωση. Ακολουθεί η αρχειοθέτηση της αναφοράς.

9. Αντιμετώπιση Καταστάσεων Έκτακτης Ανάγκης και Διαχείριση Κρίσεων

9.1. Σχέδιο Ανάκαμψης από Καταστροφή (Disaster Recovery Plan)

Στόχοι του σχεδίου ανάκαμψης από καταστροφή είναι:

- Η ελαχιστοποίηση διακοπών της κανονικής λειτουργίας.
- Ο περιορισμός της έκτασης των ζημιών και καταστροφών, και αποφυγή πιθανής κλιμάκωσης αυτών.
- Η δυνατότητα ομαλής υποβάθμισης.
- Η εγκατάσταση εναλλακτικών μέσων λειτουργίας εκ των προτέρων.
- Η εκπαίδευση, εξάσκηση και εξοικείωση του ανθρώπινου δυναμικού με διαδικασίες έκτακτης ανάγκης.
- Η δυνατότητα ταχείας και ομαλής αποκατάστασης της λειτουργίας.
- Η ελαχιστοποίηση των οικονομικών επιπτώσεων.

Με ευθύνη του Υπεύθυνου του Τμήματος Μηχανογράφησης προσδιορίζονται οι κρίσιμες εφαρμογές και τα δεδομένα των συστημάτων πληροφορικής, καθώς επίσης προσδιορίζονται και αξιολογούνται οι πιθανές απειλές γι' αυτά τα στοιχεία και προγράμματα.

Κατόπιν, επιλέγονται συγκεκριμένα μέτρα και συντάσσεται ένα σχέδιο συγκεκριμένων ενεργειών για την ανάκτηση των δεδομένων αυτών και την αντιμετώπιση μίας έκτακτης κατάστασης. Το σχέδιο αυτό ενημερώνεται με τυχόν προσθήκες ή και αλλαγές και ελέγχεται από τον Υπεύθυνο του Τμήματος Μηχανογράφησης του Ταμείου σε περιοδική βάση.

9.2. Απώλειες σε ένα Πληροφοριακό Σύστημα

Οι απώλειες που μπορούν να συμβούν σε ένα Π.Σ. μπορεί να είναι είτε ηθελημένες, δηλαδή ο μη εξουσιοδοτημένος χρήστης γνωρίζει τα αποτελέσματα των ενεργειών του, είτε αθέλητες όταν δεν τα γνωρίζει, και μπορούν να ταξινομηθούν σε τρεις κατηγορίες.

Όταν ο Η/Υ είναι εκτός ενέργειας και οι υπηρεσίες που παρέχει διακόπτονται, αυτό μπορεί να οφείλεται:

- Προσωρινή Διακοπή εξαιτίας πτώσης του ηλεκτρικού ρεύματος. Η αντιμετώπιση διενεργείται με προεγκατάσταση UPS σε όλο το δίκτυο του υπολογιστών του Ταμείου και με ηλεκτροπαραγωγικό ζεύγος (γεννήτριες παροχής ηλεκτρικού ρεύματος), οι οποίες συνδέονται αυτόματα στο δίκτυο αν και όταν παραστεί ανάγκη (UPS, Uninterrupted Power Supply) .
- Αδυναμία Σύνδεσης με τον κεντρικό server εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου. Το πρόβλημα αυτό είναι ιδιαίτερα σοβαρό σε αποκεντρωμένα Πληροφοριακά Συστήματα που λειτουργούν όμως με συγκεντρωτική μέθοδο επεξεργασίας.
- Πρόβλημα Υλικού, εξαιτίας ανθρώπινου λάθους ή πλημμελούς συντήρησης.
- Πρόβλημα Λογισμικού, εξαιτίας ανθρώπινου λάθους ή επαγγελματικής ανεπάρκειας. Σε ό,τι αφορά την προμήθεια τυποποιημένων εφαρμογών, η πιο καλή αντιμετώπιση είναι η εγγύηση διαρκούς καλής λειτουργίας και ο μακρύς χρόνος παράλληλης λειτουργίας της νέας εφαρμογής με το χειρόγραφο ή αυτοματοποιημένο σύστημα που αντικατέστησε.

9.3. Διαχείριση Κρίσεων

Ως περιστατικό ορίζεται μία παραβίαση ασφάλειας σε έναν ή περισσότερους Πληροφοριακούς Πόρους του Ταμείου. Είναι ένα επιζήμιο γεγονός μέσω του οποίου οι προδιαγραφές ασφάλειας πληροφοριών μπορεί να απειληθούν, για παράδειγμα, με απώλεια εμπιστευτικότητας, ακεραιότητας ή και καταστροφής δεδομένων, διακοπή ή άρνηση εξυπηρέτησης του συστήματος, μη εξουσιοδοτημένη χρήση πόρων κ.λπ. Κάποια παραδείγματα περιστατικών ή/και επιπτώσεων των περιστατικών θεωρούνται τα παρακάτω:

- Απώλεια εμπιστευτικότητας – μπορεί να προκληθεί από κακόβουλο εξωτερικό χρήστη που προσπελαύνει ή υποκλέπτει πληροφορίες διαβαθμισμένες ως εσωτερικής χρήσης, απόρρητες ή εμπιστευτικές, ή από μη εξουσιοδοτημένο υπάλληλο που υποκλέπτει απόρρητες ή εμπιστευτικές πληροφορίες. Καταστροφή δεδομένων – μπορεί να προκληθεί από ιό, κακόβουλο πρόγραμμα ή κακόβουλο χρήστη και μπορεί να επηρεάσει δεδομένα, στοιχεία ελέγχου και άλλες εμπιστευτικές ή απόρρητες πληροφορίες.
- Απώλεια ακεραιότητας, υποβάθμιση ή άρνηση εξυπηρέτησης του συστήματος, (συμπεριλαμβανομένων π.χ. του χρόνου απόκρισης, της αξιοπιστίας, λανθασμένων υπολογισμών, λανθασμένων διαδρομών των δεδομένων, αυξημένη μη διαθεσιμότητα κ.λπ.) ενδέχεται να προκληθεί εάν ένα πρόγραμμα μολυνθεί από ιό, ένας κακόβουλος χρήστης απενεργοποιήσει το σύστημα, ένα δικτυακό worm υπερπληρώσει το εύρος ζώνης (bandwidth), μία αδυναμία του συστήματος αποτελέσει αντικείμενο εκμετάλλευσης. Επίσης, αρνητικές συνέπειες μπορεί να προκληθούν από κακόβουλο εσωτερικό / εξωτερικό χρήστη που απέκτησε ή προσπαθεί να αποκτήσει πρόσβαση.
- Απώλεια ακεραιότητας των δεδομένων – μπορεί να προκληθεί από χρήστη που πραγματοποιεί συναλλαγές όντας μη εξουσιοδοτημένος, από έναν εισβολέα που τροποποιεί ή δημιουργεί συναλλαγές, ή από άτομα που παγιδεύουν (trap) τις εγγραφές (records) δεδομένων.
- Μη εξουσιοδοτημένη χρήση των Πληροφοριακών Πόρων.

- Άλλου είδους επιθέσεις – οποιαδήποτε υπαρκτή ή υποτιθέμενη διείσδυση στα συστήματα ασφάλειας του Ταμείου.

Σε περίπτωση περιστατικού ασφάλειας, ο Υπεύθυνος του Τμήματος Μηχανογράφησης αναλαμβάνει την διεύθυνση και καθοδήγηση των απαραίτητων υπηρεσιών του Ταμείου για να εξασφαλίσει ότι έχουν καθοριστεί οι κατάλληλοι επιχειρησιακοί πόροι προκειμένου να διερευνηθούν οι λόγοι εμφάνισης του περιστατικού και για το περιορισμό των ενδεχόμενων ζημιών. Τα Τμήματα του Ταμείου είναι υποχρεωμένα να προμηθεύσουν όποιους πόρους αιτηθεί ο Υπεύθυνος του Τμήματος Μηχανογράφησης, ανεξαρτήτως του βαθμού επίπτωσης που επέφερε το περιστατικό στο εκάστοτε τμήμα. Η Διοίκηση του Ταμείου, οι διαχειριστές συστημάτων καθώς και άλλα μέλη του προσωπικού ενδέχεται να κληθούν από τον Υπεύθυνο του Τμήματος Μηχανογράφησης ώστε να βοηθήσουν κατά τη διάρκεια περιορισμού του περιστατικού ασφάλειας.

Η αποτελεσματική διαχείριση περιστατικών ασφάλειας απαιτεί τη συμμετοχή του συνόλου του Ταμείου. Απαιτεί τη συνεργασία όλων των χρηστών, ώστε να εξασφαλισθεί ότι τα περιστατικά αναφέρονται και επιλύονται και ότι η προηγούμενη εμπειρία χρησιμοποιείται για να εφαρμοστούν μέτρα ασφάλειας που θα αποτρέψουν μελλοντικά περιστατικά. Για να είναι αποτελεσματικό το Ταμείο σε περιπτώσεις περιστατικών ασφάλειας, ενημερώνεται για το πώς να αναγνωρίζει και να προβαίνει στη διάγνωση ενός περιστατικού. Όσο συντομότερα αναγνωριστεί ένα περιστατικό, τόσο ταχύτερα μπορεί να τεθεί υπό έλεγχο.

10. Έλεγχοι αδυναμιών Λειτουργικών Συστημάτων

Τα πληροφοριακά συστήματα του Ταμείου υποβάλλονται σε τακτά χρονικά διαστήματα σε έλεγχο αδυναμιών.

Ο Υπεύθυνος του Τμήματος Μηχανογράφησης είναι αρμόδιος να κατανείμει και να αποφασίσει για τους κατάλληλους πόρους του Ταμείου που θα χρησιμοποιηθούν για την διενέργεια των ελέγχων αδυναμιών των λειτουργικών συστημάτων / εφαρμογών. Επίσης, είναι υπεύθυνος για την διευθέτηση των ευρημάτων που προήλθαν από τον έλεγχο αδυναμιών των λειτουργικών συστημάτων.

Ο Υπεύθυνος του Τμήματος Μηχανογράφησης είναι αρμόδιος για την ανάπτυξη, αξιολόγηση, παρακολούθηση και τήρηση του ενημερώσεων ελέγχου αδυναμιών. Η διόρθωση των αδυναμιών πρέπει να διενεργείται σύμφωνα με το επίπεδο αδυναμιών των λειτουργικών συστημάτων του κάθε συστήματος και με το Προφίλ Επικινδυνότητάς του προκειμένου να καθορίσει το Επίπεδο Προτεραιότητας για την διόρθωση των αδυναμιών του.

Σε συνέχεια της αναγνώρισης των αδυναμιών και της επιλογής των μεθόδων διόρθωσης, διαρκείς ενέργειες Διαχείρισης Αδυναμιών εκτελούνται ώστε να εξασφαλισθεί ότι οι επιλεγμένες μέθοδοι διόρθωσης εκτελούνται σωστά, διευθετώντας τις αδυναμίες των πληροφοριακών συστημάτων καταλλήλως.

Ο Υπεύθυνος του Τμήματος Μηχανογράφησης είναι αρμόδιος για την παρακολούθηση της διόρθωσης και των ελέγχων.