Μαρούσι, 16-09-2024

ΑΠ: 1125/17

ΑΠΟΦΑΣΗ

Έγκριση της «Πολιτικής Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα»

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ),

Έχοντας υπόψη:

1. Τις διατάξεις:

1.1 του Ν. 4070/2012 «*Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις*» (ΦΕΚ 82/Α/2012), όπως ισχύει τροποποιηθείς,

1.2 του Ν. 4053/2012 *«Ρύθμιση λειτουργίας της ταχυδρομικής αγοράς, θεμάτων ηλεκτρονικών επικοινωνιών και άλλες διατάξεις»* (ΦΕΚ 44/Α/2012), όπως ισχύει τροποποιηθείς,

1.3 του Ν. 4727/2020 *«Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) – Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.»* (ΦΕΚ 184/Α/2020),

1.4 του Κανονισμού (ΕΕ) αριθ. 679/2016 της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων ή ΓΚΠΔ),

1.5 του Ν. 4624/2019 *«Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις»* (ΦΕΚ 137/Α/2019),

1.6 του Ν. 4577/2018 *«Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις»* (ΦΕΚ 199/ Α' /03-12-2018), όπως ισχύει,

Digitally signed by SPYRIDON SYNDONAS
Date: 2024.09.30 06:40:31 EEST
Γραμματεία Ολομέλειας της ΕΕΤΤ

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

1.7 του Ν. 4961/2022 «*Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις*», (ΦΕΚ 146/Α'/27-7-2022),

1.8 του Ν. 5002/2022 «*Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών*», (ΦΕΚ 228/Α΄/2022),

2. Την ΑΠ 996/08/22-06-2021 Απόφαση της ΕΕΤΤ «*Έγκριση Οργανισμού της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων*» (ΦΕΚ 3367/Β΄/2021),

3. Την ΑΠ 1004/40/30-8-2021 Απόφαση της ΕΕΤΤ «*Κανονισμός Λειτουργίας της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)*» (ΦΕΚ 4660/Β΄/8-10-2021), όπως ισχύει τροποποιηθείσα με την ΑΠ 1062/18/24-01-2023 (ΦΕΚ 947/Β΄/2023),

4. Την εγκεκριμένη από τον Πρόεδρο της ΕΕΤΤ «*Πολιτική Ασφαλείας της ΕΕΤΤ, έκδοση 1.0*» με αριθ. πρωτ. 278/1-6-2018,

5. Την ΑΠ 989/25/26-04-2021 Απόφαση της ΕΕΤΤ «*Έγκριση της εφαρμογής της αναθεωρημένης "Πολιτικής Αποδεκτής Χρήσης των Πληροφοριακών Αγαθών της ΕΕΤΤ*"»,

6. Την ΑΠ 1048/13/24-10-2022 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών"*»,

7. Την ΑΠ 1115/11/10-06-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Πληροφοριακών Πόρων"*»,

8. Την ΑΠ 1109/13/15-4-2024 Απόφαση της ΕΕΤΤ «*Επικύρωση του Εγχειριδίου Διαδικασιών της ΕΕΤΤ*»

9. Την Εισήγηση αριθ. 37838/11-09-2024 της αρμόδιας Υπηρεσίας της ΕΕΤΤ,

και ύστερα από προφορική εισήγηση του Προέδρου της ΕΕΤΤ (Καθηγητή Κωνσταντίνου Μασσέλου),

Επειδή :

1. Η ΕΕΤΤ διαχειρίζεται, σε τακτική βάση, αλλαγές στα υπολογιστικά συστήματά της προκειμένου να προωθεί τον ψηφιακό μετασχηματισμό, να αξιοποιεί νέες τεχνολογίες και καινοτομίες, να υλοποιεί νέες απαιτήσεις λειτουργικότητας, να διορθώνει σφάλματα

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

και τεχνικές ευπάθειες, να εφαρμόζει ενημερώσεις / διορθωτικές ενέργειες, να αυξάνει την απόδοση, την ασφάλεια και αξιοπιστία των συστημάτων της, κτλ.

2. Κρίνεται σκόπιμη η υιοθέτηση μιας πολιτικής που θα ακολουθείται κατά τη μετάβαση ενός υπολογιστικού συστήματος από την υφιστάμενη σε μια άλλη βελτιωμένη κατάσταση, εξασφαλίζοντας την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα του συστήματος.
3. Σκοπός της πολιτικής αυτής θα είναι να διασφαλίσει ότι:
    - Η ΕΕΤΤ ορίζει, αναπτύσσει και εφαρμόζει τους κατάλληλους μηχανισμούς και ελέγχους για τη μείωση των περιστατικών ασφαλείας, την ικανοποίηση των κανονιστικών υποχρεώσεων και τη διαχείριση κινδύνων που σχετίζονται με αλλαγές στα ευαίσθητα ή / και κρίσιμα υπολογιστικά συστήματα,
    - οι αλλαγές εφαρμόζονται αποτελεσματικά, γρήγορα και με ελάχιστη διακοπή ή δυσλειτουργία και αναστάτωση στις υπηρεσιακές δραστηριότητες,
    - παράλληλα, γίνεται κατάλληλη διαχείριση των αλλαγών που ενδεχομένως προκύπτουν στις επηρεαζόμενες διαδικασίες, τους εμπλεκόμενους ρόλους και τις αρμοδιότητες, τους χρησιμοποιούμενους πόρους, έγγραφα κ.λπ.

Αποφασίζει :

1. **Εγκρίνει** την «*Πολιτική Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα*», η οποία στοχεύει στην ασφαλή μετάβαση των υπολογιστικών συστημάτων της ΕΕΤΤ από την υφιστάμενη σε μια βελτιωμένη κατάσταση, εξασφαλίζοντας την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των συστημάτων. Η «*Πολιτική Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα*» της ΕΕΤΤ έχει ως εξής:

« ***Πολιτική Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα***

Έκδοση: 1η

Τελευταία Ημερομηνία Ενημέρωσης: Σεπτέμβριος 2024

1. Σκοπός και πεδίο εφαρμογής

Στην παρούσα πολιτική, η Διαχείριση Αλλαγών αναφέρεται στη μετάβαση από την υφιστάμενη κατάσταση ενός υπολογιστικού συστήματος σε μια άλλη βελτιωμένη κατάσταση, εξασφαλίζοντας την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα του συστήματος. Οποιαδήποτε αναφορά σε "υπολογιστικό σύστημα" στην παρούσα υποδηλώνει συστατικά μέρη υπό τη μορφή υλικού, λογισμικού, βάσης δεδομένων, δικτύου, περιβάλλοντος εικονικοποίησης, υποδομής υποστήριξης ή / και συσκευών τελικού χρήστη ή συνδυασμού αυτών.

Η βελτιωμένη κατάσταση στην οποία επέρχεται το υπολογιστικό σύστημα μετά τις αλλαγές μπορεί να αφορά στην υλοποίηση νέων απαιτήσεων λειτουργικότητας, τη διόρθωση σφαλμάτων και τεχνικών ευπαθειών του

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

συστήματος και κατά συνέπεια τη διαχείριση ενημερώσεων / διορθωτικών ενεργειών, τη χρήση νέων τεχνολογιών, την καινοτομία, αναδιοργάνωση, αύξηση της απόδοσης, μείωση του κόστους, την ασφάλεια και αξιοπιστία του συστήματος, κτλ. ή συνδυασμό των παραπάνω.

Στο πλαίσιο αυτό, η Διαχείριση Αλλαγών στην παρούσα περιλαμβάνει προγραμματισμό, διαχείριση, έλεγχο και υποστήριξη αλλαγών, ενδεικτικά στις τεχνολογίες, τον εξοπλισμό, τον πηγαίο κώδικα, τη διαμόρφωση (ρυθμίσεις) του συστήματος, τις διαδικασίες, τους ρόλους, το υλικό τεκμηρίωσης και γενικά οτιδήποτε έχει άμεση ή έμμεση επίδραση στη λειτουργία του υπολογιστικού συστήματος και τις παρεχόμενες υπηρεσίες.

Σκοπός της Πολιτικής Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα είναι να διασφαλίσει ότι:

- *Η ΕΕΤΤ ορίζει, αναπτύσσει και εφαρμόζει τους κατάλληλους μηχανισμούς και ελέγχους για τη μείωση των περιστατικών ασφαλείας, την ικανοποίηση των κανονιστικών υποχρεώσεων και τη διαχείριση κινδύνων που σχετίζονται με αλλαγές στα ευαίσθητα ή / και κρίσιμα υπολογιστικά συστήματα,*
- *οι αλλαγές των υπολογιστικών συστημάτων εφαρμόζονται αποτελεσματικά και γρήγορα και με ελάχιστη διακοπή ή δυσλειτουργία και αναστάτωση στις υπηρεσιακές δραστηριότητες,*
- *παράλληλα, γίνεται κατάλληλη διαχείριση των αλλαγών που ενδεχομένως προκύπτουν στις επηρεαζόμενες διαδικασίες, τους εμπλεκόμενους ρόλους και τις αρμοδιότητες, τους χρησιμοποιούμενους πόρους, έγγραφα κ.λπ.*

Η πολιτική αυτή ισχύει για τους χρήστες των οποίων οι δραστηριότητες εργασίας σχετίζονται με τον κύκλο ζωής των υπολογιστικών συστημάτων και καλύπτουν πτυχές ασφάλειας που σχετίζονται με:

- *την υλοποίηση των αλλαγών στην υποδομή των υπολογιστικών συστημάτων της ΕΕΤΤ (υλικό και λογισμικό),*
- *την υλοποίηση των αλλαγών στα υπολογιστικά συστήματα της ΕΕΤΤ που φιλοξενούνται στις εγκαταστάσεις Τρίτων Μερών και τα οποία συστήματα διαχειρίζεται η ΕΕΤΤ,*
- *την υλοποίηση των αλλαγών στα υπολογιστικά συστήματα της ΕΕΤΤ που φιλοξενούνται σε εγκαταστάσεις Τρίτων Μερών και τα οποία συστήματα διαχειρίζονται τα Τρίτα Μέρη.*

Επισημαίνεται ότι μια αλλαγή υπολογιστικού συστήματος δεν πρέπει να συγχέεται με:

- *την ένταξη σε λειτουργία ενός υπολογιστικού συστήματος ή την ανάπτυξη ενός νέου πληροφοριακού συστήματος ή εφαρμογής ή module, που εμπίπτουν στην πολιτική της ΕΕΤΤ περί προμήθειας και ανάπτυξης συστημάτων,*
- *την προμήθεια ενός υπολογιστικού συστήματος την οποία χειρίζεται το Τμήμα Προμηθειών και Διοικητικής Μέριμνας ή/και η Διεύθυνση Ψηφιακής Διακυβέρνησης και εμπίπτει στην πολιτική της ΕΕΤΤ για την προμήθεια και ανάπτυξη συστημάτων.*

2. Γενικές Έννοιες

2.1 Κατηγορίες Αλλαγών στα Υπολογιστικά Συστήματα

Οι αλλαγές στα υπολογιστικά συστήματα που αποτελούν αντικείμενο της παρούσας διακρίνονται στις ακόλουθες κατηγορίες.

«Τυπικές» (standard changes) είναι οι αλλαγές περιορισμένου ρίσκου που επαναλαμβάνονται τακτικά και επαναλαμβανόμενα και ουσιαστικά δεν απαιτούν ιδιαίτερες εγκρίσεις προκειμένου να υλοποιηθούν. Ενδεικτικά παραδείγματα είναι η προσθήκη μνήμης ή χώρου αποθήκευσης, η αντικατάσταση ενός προβληματικού δρομολογητή με έναν όμοιο που λειτουργεί, η δημιουργία στιγμιότυπου μιας βάσης δεδομένων κτλ.

«Κανονικές» (normal changes) είναι μη επείγουσες αλλαγές, οι οποίες δεν είναι «τυπικές», συνηθισμένες και επαναλαμβανόμενες και δεν έχουν μία γνωστή ή προ-συμφωνημένη διαδικασία διαχείρισης. Ανάλογα την περίπτωση, ενδέχεται να ενέχουν μικρούς, μεσαίους ή μεγάλους κινδύνους, αλλά παρέχεται ο απαιτούμενος χρόνος για την αξιολόγηση της αλλαγής, την εκτίμηση των κινδύνων, τον προγραμματισμό της υλοποίησης και τη διαχείριση της εγκριτικής διαδικασίας πριν την εφαρμογή αυτών των αλλαγών. Ενδεικτικά παραδείγματα είναι η αναβάθμιση σε ένα νέο σύστημα διαχείρισης περιεχομένου, η επέκταση του διαδικτυακού τόπου ή της γνωσιακής πύλης (portal) ή η μετάβαση στο G-Cloud.

«Επείγουσες ή Έκτακτης Ανάγκης» (emergency changes) είναι αλλαγές που εγείρονται από απροσδόκητα συμβάντα, σφάλματα ή απειλές, επιφέρουν σημαντικές συνέπειες στις υπηρεσιακές λειτουργίες και πρέπει να αντιμετωπιστούν κατεπειγόντως ώστε να αποκατασταθεί άμεσα η κανονική δραστηριότητα της ΕΕΤΤ και η παροχή υπηρεσιών. Οι αλλαγές αυτές πρέπει να πραγματοποιηθούν εκτάκτως και μέσα σε ένα αυστηρό χρονοδιάγραμμα, καθώς η όποια καθυστέρηση αυξάνει τους κινδύνους. Επομένως, απαιτείται ταχεία

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

αξιολόγηση, έγκριση και εφαρμογή. Ενδεικτικά παραδείγματα είναι η εφαρμογή ενός security patch, δηλαδή μιας διόρθωσης ασφαλείας, η διακοπή λειτουργίας ενός διακομιστή, η αντιμετώπιση ενός σημαντικού περιστατικού ασφαλείας.

Η κατηγοριοποίηση της αλλαγής σε τυπική, κανονική ή επείγουσα, εξαρτάται από παράγοντες όπως ο ίδιος ο Οργανισμός, οι διαδικασίες του και η ανοχή κινδύνου που επιδεικνύει. Η κάθε κατηγορία αλλαγών απαιτεί διαφορετική διαχείριση, όπως καθίσταται προφανές από τα παραπάνω. Έτσι, οι τυπικές αλλαγές υλοποιούνται και εφαρμόζονται μέσω απλοποιημένων, συνοπτικών και προκαθορισμένων ροών εργασίας χωρίς απαιτητικές διαδικασίες αξιολόγησης, προγραμματισμού, έγκρισης και εφαρμογής.

Οι κανονικές αλλαγές μπορούν να ακολουθήσουν την κανονική συνήθη εφαρμογή της διαδικασίας διαχείρισης αλλαγών, σε αναλογία και με τους κινδύνους που ενέχουν. Υψηλού ρίσκου αλλαγές μπορεί να απαιτούν εκτεταμένη διαδικασία αξιολόγησης κινδύνων και έγκριση μέσω Απόφασης από την Ολομέλεια ή τη Διοίκηση. Χαμηλού ρίσκου αλλαγές μπορούν να εγκριθούν με ένα ταχύτερο χρονοδιάγραμμα από κάποιον που έχει εξουσιοδοτηθεί για το σκοπό αυτό ή μέσω αυτοματοποιημένων ελέγχων και αξιολόγησης από αρμόδιο προσωπικό της ΕΕΤΤ.

Οι επείγουσες αλλαγές απαιτούν ευέλικτες εγκριτικές διαδικασίες, για να επιτυγχάνεται ταχεία αξιολόγηση, έγκριση και εφαρμογή. Ενδεικτικό παράδειγμα αποτελεί η εφαρμογή αλλαγών μετά από περιστατικό ασφαλείας (βλ. Πολιτική Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών).

Γενικότερα, η απόφαση σχετικά με το εάν θα εφαρμοστεί πλήρως η διαδικασία διαχείρισης αλλαγών βασίζεται στο βαθμό επιπτώσεων και στον επείγοντα ή όχι χαρακτήρα της αλλαγής. Πάντως, στόχος της παρούσας είναι μια σύγχρονη διαχείριση αλλαγών όπου οι διαδικασίες είναι όσο το δυνατόν πιο απλοποιημένες, αυτοματοποιημένες και λιγότερο χρονοβόρες και γραφειοκρατικές.

2.2 Διαδικασία Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα

Η ΕΕΤΤ διαθέτει και χρησιμοποιεί μια τυπική, δομημένη και τεκμηριωμένη Διαδικασία Διαχείρισης Αλλαγών για την εφαρμογή των αλλαγών στα υπολογιστικά συστήματά της. Η διαδικασία αυτή λαμβάνει υπόψη τους ανθρώπινους πόρους, τις διεργασίες και τα συστήματα που θα επηρεαστούν από τις αλλαγές και περιλαμβάνει, κυρίως, τα ακόλουθα βήματα:

- *Υποβολή ψηφιακού αιτήματος αλλαγής από στέλεχος της ΕΕΤΤ (συμπεριλαμβανομένων και των στελεχών της Διεύθυνσης Ψηφιακής Διακυβέρνησης) σε ειδική εφαρμογή διαχείρισης αιτημάτων. Η υποβολή του αιτήματος αποτελεί το έναυσμα της διαδικασίας. Κατόπιν το αίτημα, μέσω της εφαρμογής, προωθείται κατάλληλα στους αρμόδιους για την αντιμετώπιση/επίλυσή του*
- *Αξιολόγηση του αιτήματος αλλαγής, π.χ. από τον Υπεύθυνο Ασφάλειας Πληροφοριών (CISO), τον Υπεύθυνο Προστασίας Δεδομένων (DPO) κτλ., ανάλογα με την περίπτωση*
- *Ανάπτυξη του σχεδίου υλοποίησης της αλλαγής (προτεραιότητες, χρονοδιάγραμμα, αναμενόμενα αποτελέσματα, κατανομή των πόρων, ρόλοι, υπεύθυνοι, αρμοδιότητες, σχέδιο δοκιμών, σχέδιο επαναφοράς σε περίπτωση αποτυχίας, σχέδιο επικοινωνίας της αλλαγής κτλ.)*
- *Έγκριση της αλλαγής, ανάλογα με την περίπτωση, π.χ. από τους αρμόδιους Προϊσταμένους, τη Διοίκηση, την Ολομέλεια κτλ.*
- *Υλοποίηση της αλλαγής, τεκμηριώνοντας τη διαδικασία και τα ενδιάμεσα αποτελέσματά της. Η υλοποίηση παρακολουθείται και ελέγχεται από τους αρμόδιους. Στην περίπτωση αποκλίσεων από το σχεδιασμό, λαμβάνονται διορθωτικές ενέργειες*
- *Ανασκόπηση και ανάλυση της αλλαγής, καταγράφοντας και επικοινωνώντας την αποτελεσματικότητα και απόδοση της αλλαγής ως προς την επίτευξή της, τον πραγματοποιηθέντα χρόνο υλοποίησης σε σχέση με την αρχική εκτίμηση, το απολογιστικό κόστος σε σχέση με τον προϋπολογισμό κτλ.*
- *Καταγραφή της επίλυσης στην ειδική εφαρμογή διαχείρισης αιτημάτων, ενημέρωση του αιτούντα και των λοιπών εμπλεκόμενων και ολοκλήρωση / κλείσιμο της εκκρεμότητας και της διαδικασίας διαχείρισης της αλλαγής.*

Γενικά, η ΕΕΤΤ απλοποιεί ευέλικτα τις διαδικασίες διαχείρισης των αλλαγών, όπου αυτό είναι εφικτό. Αξιοποιεί προκαθορισμένες διαδικασίες για τις Τυπικές αλλαγές και συνοπτικές διαδικασίες για τις αλλαγές Έκτακτης Ανάγκης εάν δεν υπάρχει αρκετός χρόνος. Ενδεικτικά, μπορεί να μην προηγηθεί μια εκτεταμένη τυπική αξιολόγηση ή έγκριση αιτήματος ή να μην υλοποιηθεί πλήρες σχέδιο δοκιμών για μια κατεπείγουσα ή μικρής έκτασης αλλαγή.

Η διαδικασία διαχείρισης αλλαγών πρέπει να λαμβάνει υπόψη τα σχέδια της ΕΕΤΤ για την επιχειρησιακή συνέχεια και την ανάκαμψη από καταστροφές, ώστε να διασφαλίζεται η ελάχιστη διακοπή των λειτουργιών, η

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

αποδοτική χρήση των πόρων για την υλοποίηση των αλλαγών και η εναρμόνιση των σχεδίων αυτών με τις νέες υπηρεσίες.

2.3 Μητρώο Αλλαγών

Η ΕΕΤΤ τηρεί Μητρώο Πληροφοριακών Πόρων, το οποίο περιλαμβάνει τις πληροφορίες για κάθε πληροφοριακό πόρο της, όπως περιγράφεται στην Πολιτική Διαχείρισης Πληροφοριακών Πόρων. Το Μητρώο αυτό είναι απαραίτητο για την αποτελεσματική εφαρμογή της Διαδικασίας Διαχείρισης Αλλαγών.

Για κάθε επιχειρησιακή εφαρμογή του Μητρώου Πληροφοριακών Πόρων της ΕΕΤΤ πρέπει να τηρείται λεπτομερές αρχείο (μητρώο) των αλλαγών (είτε σε έντυπη είτε σε ηλεκτρονική μορφή), το οποίο να περιλαμβάνει:

- *Αιτήματα αλλαγών*
- *Εγκρίσεις των αλλαγών*
- *Αποτελέσματα δοκιμών και υλοποιήσεων*
- *Ημερομηνίες υλοποίησης / εγκατάστασης*
- *Δοκιμές αποδοχής*

2.4 Επικοινωνία των Αλλαγών στα εμπλεκόμενα μέρη

Οι προγραμματισμένες αλλαγές που επηρεάζουν τη λειτουργία των πληροφοριακών πόρων της ΕΕΤΤ πρέπει να γνωστοποιούνται έγκαιρα στα εμπλεκόμενα μέρη που ενδέχεται να επηρεαστούν από την αλλαγή (όπως για παράδειγμα στην περίπτωση διακοπής λειτουργίας συστήματος). Η γνωστοποίηση γίνεται μέσω ηλεκτρονικού ταχυδρομείου και με ανάρτηση στη Γνωσιακή Πύλη.

2.5 Διαχείριση Αλλαγών και Τρίτα Μέρη

Η διαχείριση των αλλαγών στα υπολογιστικά συστήματα της ΕΕΤΤ που φιλοξενούνται σε εγκαταστάσεις Τρίτων Μερών (είτε τα διαχειρίζονται Τρίτα Μέρη είτε η ίδια η ΕΕΤΤ) πρέπει να προβλέπονται στις σχετικές προκηρύξεις διαγωνισμών και στις συμβάσεις που υπογράφονται μεταξύ της ΕΕΤΤ και των Τρίτων Μερών.

3. Υποβολή, Αξιολόγηση και Έγκριση Αιτημάτων Αλλαγής

3.1 Υποβολή Αιτημάτων Αλλαγής

Τα αιτήματα αλλαγής υποβάλλονται και ανατίθενται ψηφιακά μέσω ειδικής εφαρμογής που διαχειρίζεται τα αιτήματα της ΕΕΤΤ, η οποία παρέχει την δυνατότητα συνεργασίας των εμπλεκόμενων με διαφανή τρόπο σε όλη τη ροή εργασιών (workflow). Λειτουργεί και ως γνωσιακή βάση για γνωστά σφάλματα, διαδικασίες βήμα προς βήμα, συνηθισμένα θέματα και τις λύσεις τους, η οποία εμπλουτίζεται από την ΕΕΤΤ με καθημερινή γνώση, έτσι ώστε οι έχοντες πρόσβαση να μαθαίνουν από τις προηγούμενες σχετικές εργασίες και να βελτιώνουν την αποδοτικότητα της διαχείρισης αλλαγών.

Στις περιπτώσεις που τα αιτήματα αφορούν αλλαγές σε συστήματα που τα διαχειρίζονται Τρίτα Μέρη, τότε τα αιτήματα αυτά, εφόσον είναι κρίσιμα, καταγράφονται στην ειδική εφαρμογή διαχείρισης αιτημάτων της ΕΕΤΤ, ασχέτως εάν παράλληλα καταχωρούνται και σε ειδικές εφαρμογές των Τρίτων Μερών, για λόγους πληρότητας στην παρακολούθηση των αλλαγών εντός ΕΕΤΤ, προκειμένου να τηρούνται αναλυτικά ιστορικά στοιχεία των αλλαγών και να ενημερώνεται η γνωσιακή βάση.

Κάθε αίτημα αλλαγής καταγράφεται και λαμβάνει έναν μοναδικό αριθμό αναφοράς.

Για κάθε αίτημα αλλαγής πρέπει να καταγράφεται και να τηρείται, ανάλογα με την περίπτωση:

- *Το αντικείμενο της αλλαγής*
- *Περιγραφή της αλλαγής, σε λεπτομέρεια που καθορίζεται από τα ειδικά χαρακτηριστικά της κάθε περίπτωσης*
- *Ο κύριος αιτών την αλλαγή*
- *Ο υπεύθυνος/οι υπεύθυνοι επίλυσης*
- *Τα προσδοκώμενα οφέλη*
- *Εναλλακτικές λύσεις, εφόσον υπάρχουν και είναι γνωστές*
- *Τα υπολογιστικά συστήματα που θα επηρεαστούν από την αλλαγή*

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

- *Οι υπηρεσίες που θα επηρεαστούν κατά την εφαρμογή της αλλαγής*
- *Ο εκτιμώμενος χρόνος διακοπής των σχετικών υπηρεσιών ή υπολογιστικών συστημάτων*
- *Το επίπεδο επίπτωσης και ο επείγων ή όχι χαρακτήρας της αλλαγής*
- *Απαιτούμενοι πόροι υλοποίησης*
- *Το προτεινόμενο σχέδιο επαναφοράς για την περίπτωση αποτυχίας της αλλαγής (roll-back plan)*
- *Πρόσθετοι κίνδυνοι που σχετίζονται με την αλλαγή.*

Μετά την υποβολή, το αίτημα δρομολογείται στο επόμενο εξουσιοδοτημένο άτομο μέσω ροών εργασίας βάσει των επιχειρησιακών κανόνων. Έτσι, τα αιτήματα αλλαγής χρεώνονται στο αρμόδιο Τμήμα και στον αρμόδιο υπάλληλο της Διεύθυνσης Ψηφιακής Διακυβέρνησης της ΕΕΤΤ, ο οποίος είναι υπεύθυνος για τη διεκπεραίωση του αιτήματος αλλαγής.

3.2 Αξιολόγηση των Αιτημάτων Αλλαγής και των Επιπτώσεων τους στην Ασφάλεια και Έγκριση των Αλλαγών

Τα αιτήματα αλλαγής πρέπει να αξιολογούνται από τη Διεύθυνση Ψηφιακής Διακυβέρνησης, τον Υπεύθυνο Ασφάλειας Πληροφοριακών Συστημάτων (ΥΑΠΣ) και τον Υπεύθυνο Προστασίας Δεδομένων εάν εμπλέκονται προσωπικά δεδομένα.

Η έγκριση ενός αιτήματος αλλαγής πρέπει να βασίζεται σε προκαθορισμένα κριτήρια (π.χ. την κατηγορία της αλλαγής, υπηρεσιακές απαιτήσεις, αναγκαιότητα / κρισιμότητα της αλλαγής, συνέπειες, κίνδυνοι, άλλες εναλλακτικές, επιπτώσεις στην ασφάλεια, εκτιμήσεις προϋπολογισμού, απαιτούμενοι πόροι, ρόλοι, αρμοδιότητες, αλληλεξαρτήσεις και προτεραιότητες μεταξύ αλλαγών κλπ.) και στα αποτελέσματα της αξιολόγησης του αιτήματος αλλαγής. Η εγκριτική διαδικασία περιλαμβάνει ανά περίπτωση τα κατάλληλα στελέχη της ΕΕΤΤ από την Διεύθυνση Ψηφιακής Διακυβέρνησης, από άλλες αρμόδιες Υπηρεσίες της ΕΕΤΤ και στην περίπτωση κρίσιμων αλλαγών από τη Διοίκηση ή την Ολομέλεια.

Η προτεραιοποίηση και επομένως η σειρά υλοποίησης των αλλαγών είναι απαραίτητη για την κατάλληλη κατανομή των πόρων. Το πόσο επείγουσα είναι μία συγκεκριμένη αλλαγή πρέπει να καθορίζεται με βάση το σύστημα ταξινόμησης της ΕΕΤΤ (βλ. την Πολιτική Διαχείρισης Πληροφοριακών Πόρων). Σε κάθε αλλαγή πρέπει να δίδεται προτεραιότητα ανάλογα με τον αντίκτυπο και τον επείγοντα ή όχι χαρακτήρα της αλλαγής.

Ως μέρος της διαδικασίας έγκρισης μιας αλλαγής, πριν από την εφαρμογή οποιασδήποτε αλλαγής στα ευαίσθητα ή κρίσιμα συστήματα της ΕΕΤΤ, πρέπει να διεξάγεται αξιολόγηση κινδύνων. Η αξιολόγηση κινδύνων πρέπει να υποστηρίζεται από μια ανάλυση επιχειρησιακών επιπτώσεων (Business Impact Analysis - BIA) για τον προσδιορισμό των παραγόντων που ενδέχεται να οδηγήσουν σε διακοπή ή δυσλειτουργία των επιχειρησιακών διαδικασιών της ΕΕΤΤ. Επομένως, κάθε αλλαγή πρέπει να εκτιμάται με βάση:

- *την πιθανότητα εμφάνισης του κινδύνου, και*
- *τις επιπτώσεις σε περίπτωση εμφάνισης του κινδύνου.*

Έτσι, εάν ένα σύστημα παρουσιάζει μέτριες ή υψηλές ευπάθειες ασφαλείας, τότε θα πρέπει να εξετάζεται η αντικατάστασή του παρά η περιορισμένη διαχείριση αλλαγών.

Οι αλλαγές που δεν εγκρίνονται πρέπει να ακυρώνονται / απορρίπτονται από τους αξιολογητές.

4. Δοκιμές, Υλοποίηση και Ανασκόπηση των Αλλαγών

4.1 Σχέδιο Δοκιμών και εφαρμογή του

Για κάθε αλλαγή, θα πρέπει να καταγράφεται σχέδιο δοκιμών (συμπεριλαμβανομένων δοκιμών της ασφάλειας (security testing), των μερών (unit testing), της ενσωμάτωσης (integration testing), του συστήματος (system testing), της απόδοσης (performance testing), των προσομοιώσεων ακραίων καταστάσεων (stress testing), της αποδοχής (acceptance testing) κ.λπ., ανάλογα με την περίπτωση). Με το σχέδιο δοκιμών, αποφεύγονται περιστατικά με δυσμενείς συνέπειες.

Κάθε αλλαγή πρέπει να δοκιμάζεται σε περιβάλλον δοκιμών (test environment), σύμφωνα με το σχέδιο δοκιμών, προτού εφαρμοστεί στο παραγωγικό περιβάλλον (production environment). Η μόνη επιτρεπόμενη εξαίρεση σε αυτή την πολιτική δοκιμής των αλλαγών αφορά Επείγουσες ή Έκτακτης Ανάγκης αλλαγές που πρέπει να εφαρμοστούν άμεσα. Σε αυτή την περίπτωση, οι αξιολογητές επιτρέπεται να εγκρίνουν μια εξαίρεση από τις συνήθεις εκτεταμένες δοκιμές.

Το περιβάλλον δοκιμών πρέπει να είναι απομονωμένο από το παραγωγικό σύστημα και επικαιροποιημένο. Κατά τη δοκιμή του λογισμικού, τα χρησιμοποιούμενα δεδομένα συνιστάται να είναι μη πραγματικά (dummy

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

data). Αν είναι αναγκαίο να χρησιμοποιηθούν πραγματικά δεδομένα πρέπει, κατά το δυνατόν, να είναι σε ανωνυμοποιημένη μορφή χωρίς προσωπικά δεδομένα.

4.2 Υλοποίηση των Αλλαγών στα Υπολογιστικά Συστήματα

Η κατάσταση ασφαλείας ενός υπολογιστικού συστήματος πρέπει πάντα να ελέγχεται προ της υλοποίησης σημαντικών αλλαγών στη διαμόρφωσή του (ή των επιμέρους στοιχείων του). Η ΕΕΤΤ πρέπει να αναπτύξει, να τεκμηριώσει και να διατηρεί μια ενημερωμένη, πλήρη, ακριβή και άμεσα διαθέσιμη βασική διαμόρφωση ασφαλείας για τουλάχιστον κάθε ευαίσθητο ή / και κρίσιμο υπολογιστικό σύστημα (secure configuration baseline). Οι βασικές ρυθμίσεις ασφαλείας των ευαίσθητων ή / και κρίσιμων υπολογιστικών συστημάτων πρέπει να ενημερώνονται τακτικά.

Πριν από την εφαρμογή των αλλαγών, πρέπει να λαμβάνονται αντίγραφα ασφαλείας όλων των κρίσιμων και / ή ευαίσθητων υπολογιστικών συστημάτων που επηρεάζονται από τις αλλαγές. Στη συνέχεια, οι αλλαγές υλοποιούνται μόνο από εξουσιοδοτημένο προσωπικό. Σε περίπτωση ανεπιτυχούς εφαρμογής της αλλαγής, θα εφαρμόζεται το σχετικό Σχέδιο Επαναφοράς (Roll-Back Plan).

Η υλοποίηση των αλλαγών περιλαμβάνει απαραιτήτως την τήρηση της σχετικής τεκμηρίωσης για μελλοντικές αναφορές. Παράλληλα, εξασφαλίζονται οι απατήσεις της νομοθεσίας για την προστασία των προσωπικών δεδομένων και την ασφάλεια των συστημάτων. Επανεξετάζονται και προσαρμόζονται οι όροι χρήσης, η δήλωση προστασίας προσωπικών δεδομένων, η δήλωση προσβασιμότητας, οι ρυθμίσεις και η πολιτική cookies, η μελέτη εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων (ΕΑΠΔ ή αλλιώς DPIA), η μελέτη ταξινόμησης των δεδομένων (data classification) κτλ. του συστήματος, όπου απαιτείται και σε κάθε περίπτωση πριν την ένταξη των αλλαγών σε παραγωγική λειτουργία.

Επίσης, ακολουθεί σχετική εκπαίδευση των εμπλεκόμενων μερών, ενδεχομένως μέσω εκπαίδευσης επί της εργασίας (on the job training). Στις περιπτώσεις που κρίνεται απαραίτητο, της ένταξης της αλλαγής στην παραγωγική λειτουργία μπορεί να προηγηθεί μια δοκιμαστική ή πιλοτική λειτουργία, σύμφωνα με το σχεδιασμό που έχει προηγηθεί.

4.3 Συνεχής Παρακολούθηση των Υπολογιστικών Συστημάτων που Επηρεάζονται από τις Αλλαγές

Τα υπολογιστικά συστήματα στα οποία έχουν εφαρμοστεί σημαντικές αλλαγές, πρέπει να παρακολουθούνται για παρατεταμένη χρονική περίοδο ανάλογα με το επίπεδο ταξινόμησής τους. Δηλαδή όσο πιο ευαίσθητο ή κρίσιμο έχει ταξινομηθεί ένα σύστημα, τόσο περισσότερο χρονικό διάστημα πρέπει να παρακολουθείται ως προς τη λειτουργία του μετά την εφαρμογή των αλλαγών.

Επίσης, πρέπει να διεξάγεται ανασκόπηση μετά την εφαρμογή κάθε αλλαγής που γίνεται στα υπολογιστικά συστήματα της ΕΕΤΤ, προκειμένου να αξιοποιηθεί η γνώση που αποκτήθηκε σε όλη τη διάρκεια της αλλαγής και να υποστηριχθούν μελλοντικές αλλαγές ή / και άλλες στρατηγικές ασφάλειας (π.χ. εφαρμογή βασικών ρυθμίσεων ασφαλείας σε συστήματα).

5. Ετήσιος Προγραμματισμός Αλλαγών για τα Υπολογιστικά Συστήματα

Για να είναι αποτελεσματική η διαχείριση αλλαγών ως προς την ιεράρχηση των εργασιών και την κατάλληλη κατανομή των πόρων, είναι απαραίτητος ο ετήσιος προγραμματισμός. Επομένως, οι οργανικές μονάδες πρέπει να μεριμνούν να ενημερώνουν τη Διεύθυνση Ψηφιακής Διακυβέρνησης στις αρχές του έτους, κατά το σχεδιασμό των έργων και της στοχοθεσίας τους, για τις αλλαγές που επιθυμούν να υλοποιηθούν μέσα στο έτος. Έτσι, η Διεύθυνση Ψηφιακής Διακυβέρνησης θα οργανώνει αποτελεσματικότερα τα έργα και τις εργασίες της, θα καταρτίζει τον προϋπολογισμό και τη δική της στοχοθεσία και πλάνο δράσεων. Η υποβολή έκτακτων αλλαγών απροειδοποίητα στη διάρκεια του έτους πρέπει να αποφεύγεται. Ο ετήσιος προγραμματισμός θα αναθεωρείται μέσα στο έτος εάν προκύπτει σοβαρός λόγος.

»

2. **Εντέλλεται** την κοινοποίηση της παρούσας Απόφασης στο προσωπικό της ΕΕΤΤ μέσω ανάρτησής της στη Γνωσιακή Πύλη (portal) και αποστολής της με μήνυμα ηλεκτρονικού ταχυδρομείου.
3. **Ορίζει** ότι η *«Πολιτική Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα»* συνδέεται άρρηκτα με τις υπό στοιχείο 4΄, 5΄, 6΄, 7΄ ως άνω πολιτικές ασφαλείας της ΕΕΤΤ και

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

πρέπει να εφαρμόζεται υποχρεωτικά και απαρέγκλιτα από το προσωπικό της του οποίου οι δραστηριότητες εργασίας σχετίζονται με τον κύκλο ζωής των υπολογιστικών συστημάτων.

4. **Εξουσιοδοτεί** τον Πρόεδρο της ΕΕΤΤ όπως:
    - Προβεί σε κάθε διαδικαστική ενέργεια ή έκδοση πράξης, που θα διευκολύνει την έγκαιρη και πλήρη ολοκλήρωση κάθε δράσης που αφορά στην εφαρμογή της *«Πολιτικής Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα»*.
    - Τροποποιεί την *«Πολιτική Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα»*, όποτε αυτό απαιτείται.

Ο ΠΡΟΕΔΡΟΣ

ΚΑΘΗΓΗΤΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ ΜΑΣΣΕΛΟΣ

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr