

ΔΙΑΔΙΚΑΣΙΑ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΕΧΝΟΛΟΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΩΣ ΠΡΟΣ ΤΗΝ ΑΣΦΑΛΕΙΑ

Έκδοση 1.0
Οκτώβριος 2026

Πίνακας Περιεχομένων

Άρθρο 1 5
Αντικείμενο και σκοπός 5
Άρθρο 2 5
Πεδίο εφαρμογής 5
Άρθρο 3 6
Ορισμοί 6
Άρθρο 4 7
Φύση και όρια της αξιολόγησης 7
Άρθρο 5 7
Αρχές της διαδικασίας και αρμόδια όργανα 7
Άρθρο 6 8
Υποβολή αίτησης 8
Άρθρο 7 9
Αρχικός έλεγχος της αίτησης 9
Άρθρο 8 9
Τεχνικός Φάκελος Ασφάλειας 9
Άρθρο 9 10
Πλαίσια αναφοράς και φύση της πιστοποίησης 10
Άρθρο 10 11
Σύστημα βαθμολόγησης 11
Άρθρο 11 12
Γενική κλίμακα βαθμολόγησης 12
Άρθρο 12 12
Κριτήριο 1: Αρχιτεκτονική Ασφάλειας και Μοντέλο Απειλών 12
Άρθρο 13 13
Κριτήριο 2: Ταυτοποίηση, Αυθεντικοποίηση και Έλεγχος Πρόσβασης 13
Άρθρο 14 13
Κριτήριο 3: Προστασία Δεδομένων και Κρυπτογραφία 13
Άρθρο 15 14
Κριτήριο 4: Ασφάλεια Επικοινωνιών, Δικτύων και Διεπαφών 14
Άρθρο 16 14
Κριτήριο 5: Ακεραιότητα Συστήματος, Εκτέλεσης και Λειτουργιών 14
Άρθρο 17 15
Κριτήριο 6: Καταγραφή, Ιχνηλασιμότητα και Παρακολούθηση 15

Άρθρο 18....15
Κριτήριο 7: Διαχείριση Ευπαθειών, Διαμόρφωσης και Ενημερώσεων....15
Άρθρο 19....16
Κριτήριο 8: Διαθεσιμότητα, Ανθεκτικότητα και Ανάκτηση....16
Άρθρο 20....16
Κριτήριο 9: Εξαρτήσεις, Τρίτα Συστατικά και Αλυσίδα Εφοδιασμού....16
Άρθρο 21....17
Κριτήριο 10: Ασφαλής Ανάπτυξη, Μεταβολές και Διάθεση Εκδόσεων....17
Άρθρο 22....17
Κρίσιμες Αδυναμίες....17
Άρθρο 23....18
Έκθεση Αξιολόγησης....18
Άρθρο 24....18
Συμπληρωματικά στοιχεία....18
Άρθρο 25....19
Ανεξάρτητη επανεξέταση....19
Άρθρο 26....19
Απόφαση πιστοποίησης....19
Άρθρο 27....20
Πιστοποιητικό Τεκμηριωτικής Αξιολόγησης Ασφάλειας Τεχνολογικού Συστήματος ΚΕΜΕΑ....20
Άρθρο 28....20
Διάρκεια ισχύος, Κατάσταση Συστήματος και επιτήρηση....20
Άρθρο 29....22
Ουσιώδεις Μεταβολές....22
Άρθρο 30....23
Αναστολή, ανάκληση, παραίτηση και αναφορές τρίτων....23
Άρθρο 31....23
Ενστάσεις....23
Άρθρο 32....24
Εμπιστευτικότητα....24
Άρθρο 33....25
Μητρώο πιστοποιημένων Συστημάτων....25
Άρθρο 34....25
Χρήση της πιστοποίησης....25
Άρθρο 35....26

Οικονομικοί όροι....26
Άρθρο 36....27
Τήρηση αρχείων....27
Άρθρο 37....27
Ερμηνεία της Βαθμολογίας Ασφάλειας....27
Άρθρο 38....28
Έγκριση, έναρξη ισχύος και δημοσιοποίηση....28

Άρθρο 1

Αντικείμενο και σκοπός

1. Η παρούσα καθορίζει τη διαδικασία που εφαρμόζει το Κέντρο Μελετών Ασφάλειας, εφεξής ΚΕΜΕΑ, για την πιστοποίηση Τεχνολογικών Συστημάτων ως προς την ασφάλειά τους, στο πλαίσιο της περ. ια΄ της παρ. 2 του άρθρου 3 του ν. 3387/2005, όπως η περίπτωση αυτή αντικαταστάθηκε με το άρθρο 105 του ν. 5301/2026 και ισχύει.

2. Η πιστοποίηση αποσκοπεί στην αξιολόγηση του επιπέδου ασφάλειας συγκεκριμένου Τεχνολογικού Συστήματος, όπως αυτό προκύπτει από την υποβαλλόμενη τεκμηρίωση, και ιδίως της ικανότητάς του να προστατεύει την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την αυθεντικότητα δεδομένων, λειτουργιών και υπηρεσιών.

3. Στην παρούσα υπάγονται Τεχνολογικά Συστήματα που χρησιμοποιούνται ή προορίζονται να χρησιμοποιηθούν από φορείς, οργανισμούς ή επιχειρήσεις του δημόσιου ή ιδιωτικού τομέα, στο μέτρο που τα μέτρα και οι μηχανισμοί ασφάλειάς τους δύνανται να συμβάλλουν στην ασφάλεια των φορέων, οργανισμών ή επιχειρήσεων αυτών.

4. Η αξιολόγηση μπορεί να αφορά ολόκληρο Τεχνολογικό Σύστημα ή σαφώς προσδιορισμένο τμήμα, έκδοση, διαμόρφωση ή αρχιτεκτονική αυτού.

5. Η πιστοποίηση αφορά αποκλειστικά τα τεχνολογικά μέτρα, τους μηχανισμούς και τις ιδιότητες ασφάλειας του Αντικειμένου Αξιολόγησης.

6. Η παρούσα αφορά αποκλειστικά την πιστοποίηση Τεχνολογικών Συστημάτων ως προς την ασφάλεια και δεν εφαρμόζεται στην πιστοποίηση διαδικασιών, μελετών, σχεδίων ή άλλων αντικειμένων, για τα οποία το ΚΕΜΕΑ δύναται να θεσπίζει αυτοτελείς διαδικασίες.

Άρθρο 2

Πεδίο εφαρμογής

1. Στην παρούσα μπορούν να υπαχθούν ιδίως:

α) εφαρμογές λογισμικού,
β) πληροφοριακά συστήματα,
γ) διαδικτυακές και κινητές εφαρμογές,
δ) συστήματα CRM, ERP και λοιπά επιχειρησιακά συστήματα,
ε) βάσεις δεδομένων και συστήματα διαχείρισης δεδομένων,
στ) υπολογιστικές, δικτυακές και τηλεπικοινωνιακές πλατφόρμες,
ζ) συστήματα και υπηρεσίες υπολογιστικού νέφους,
η) συσκευές και τεχνολογικός εξοπλισμός,
θ) ενσωματωμένα συστήματα,
ι) συστήματα IoT,
ια) συστήματα OT και βιομηχανικού ελέγχου,
ιβ) συστήματα βιντεοεπιτήρησης, ελέγχου πρόσβασης και λοιπά συστήματα φυσικής ασφάλειας,
ιγ) μικτά συστήματα που συνδυάζουν υλικό εξοπλισμό, λογισμικό, υλικολογισμικό, δίκτυα ή υπηρεσίες,

ιδ) κάθε άλλο Τεχνολογικό Σύστημα που πληροί τις προϋποθέσεις της παρ. 3 του άρθρου 1.

2. Η πιστοποίηση μπορεί να αφορά Σύστημα που βρίσκεται σε παραγωγική λειτουργία, Σύστημα υπό ανάπτυξη, Σύστημα του οποίου έχει ολοκληρωθεί ο σχεδιασμός ή συγκεκριμένη τεχνολογική αρχιτεκτονική, εφόσον το ακριβές Αντικείμενο Αξιολόγησης προσδιορίζεται με σαφήνεια. Η συγκεκριμένη τεχνολογική αρχιτεκτονική αντιμετωπίζεται, για τους σκοπούς της παρούσας, ως Σύστημα στο στάδιο του σχεδιασμού.

Άρθρο 3

Ορισμοί

Για την εφαρμογή της παρούσας νοούνται ως:

1. «Τεχνολογικό Σύστημα»: οργανωμένο σύνολο λογισμικού, υλικού εξοπλισμού, υλικολογισμικού, δικτυακών στοιχείων, δεδομένων, διεπαφών και συναφών τεχνικών λειτουργιών, ανεξαρτήτως του αν συνυπάρχουν όλα τα ανωτέρω στοιχεία.

2. «Αντικείμενο Αξιολόγησης»: το υπό αξιολόγηση Τεχνολογικό Σύστημα στο σύνολό του ή τμήμα, έκδοση, διαμόρφωση ή αρχιτεκτονική του, που υποβάλλεται προς πιστοποίηση.

3. «Αιτών»: το φυσικό ή νομικό πρόσωπο που ζητεί την πιστοποίηση.

4. «Τεχνικός Φάκελος Ασφάλειας»: το σύνολο των τεχνικών πληροφοριών, εγγράφων, διαγραμμάτων, προδιαγραφών, δηλώσεων και λοιπών τεκμηρίων που τίθενται υπόψη του ΚΕΜΕΑ.

5. «Τεκμηριωτική Αξιολόγηση Ασφάλειας»: η αξιολόγηση του Αντικειμένου Αξιολόγησης βάσει του Τεχνικού Φακέλου Ασφάλειας και κάθε συμπληρωματικού στοιχείου που υποβάλλεται στο ΚΕΜΕΑ.

6. «Βαθμολογία Ασφάλειας»: η συνολική βαθμολογία από μηδέν έως εκατό μονάδες που προκύπτει από την εφαρμογή των δέκα Κριτηρίων Ασφάλειας.

7. «Κρίσιμη Αδυναμία»: αδυναμία η οποία, όπως προκύπτει από τα στοιχεία που τέθηκαν υπόψη του ΚΕΜΕΑ ή από δημόσια διαθέσιμες πληροφορίες, δημιουργεί άμεσο ή ιδιαιτέρως σοβαρό κίνδυνο σοβαρής παραβίασης κρίσιμων δεδομένων ή λειτουργιών. Κρίσιμα είναι τα δεδομένα και οι λειτουργίες που προσδιορίζονται ως τέτοια στον Τεχνικό Φάκελο Ασφάλειας ή, με ειδική αιτιολόγηση, στην Έκθεση Αξιολόγησης. Ενδεικτικές περιπτώσεις και κανόνες εφαρμογής ορίζονται στο άρθρο 22.

8. «Ουσιώδης Μεταβολή»: μεταβολή στην αρχιτεκτονική, διαμόρφωση ή λειτουργία του Συστήματος που δύναται να επηρεάσει ουσιωδώς την αξιολόγηση της ασφάλειάς του.

9. «Κάτοχος»: ο Αιτών στον οποίο έχει χορηγηθεί πιστοποιητικό κατά την παρούσα.

10. «Κατάσταση Συστήματος»: η ένδειξη του σταδίου υλοποίησης του Αντικειμένου Αξιολόγησης στο πιστοποιητικό και στο Μητρώο. Η ένδειξη είναι «Υπό ανάπτυξη» όταν η αξιολόγηση αφορά σχεδιασμό, τεχνολογική αρχιτεκτονική ή Σύστημα του οποίου η υλοποίηση δεν έχει ολοκληρωθεί. Η ένδειξη είναι «Υλοποιημένο» όταν είτε (α) η υλοποίηση έχει ήδη ολοκληρωθεί κατά την αρχική αξιολόγηση και η αξιολόγηση διενεργείται βάσει τεκμηρίων της συγκεκριμένης υλοποιημένης έκδοσης, είτε (β) μετά τη συμπληρωματική τεκμηριωτική αξιολόγηση του άρθρου 28 παρ. 6 προκύπτει από τα προσκομισθέντα στοιχεία ότι η υλοποιημένη έκδοση αντιστοιχεί στην πιστοποιημένη αρχιτεκτονική και στα αξιολογημένα μέτρα και μηχανισμούς ασφάλειας. Η ένδειξη

«Υλοποιημένο» δεν συνιστά ανεξάρτητη τεχνική ή εργαστηριακή επαλήθευση της πραγματικής υλοποίησης.

11. «Κριτήρια Ασφάλειας»: τα δέκα κριτήρια των άρθρων 12 έως 21, βάσει των οποίων βαθμολογείται το Αντικείμενο Αξιολόγησης.

12. «Μητρώο»: το μητρώο πιστοποιητικών που τηρεί το ΚΕΜΕΑ κατά το άρθρο 33.

Άρθρο 4

Φύση και όρια της αξιολόγησης

1. Η πιστοποίηση πραγματοποιείται βάσει τεκμηριωτικής αξιολόγησης.

2. Η αξιολόγηση βασίζεται στα στοιχεία που υποβάλλονται από τον αιτούντα και σε τυχόν συμπληρωματικά στοιχεία που ζητεί το ΚΕΜΕΑ, καθώς και, για τη διαπίστωση Κρίσιμης Αδυναμίας, σε δημόσια διαθέσιμες πληροφορίες κατά την παρ. 7 του άρθρου 3.

3. Το ΚΕΜΕΑ αξιολογεί την τεχνική επάρκεια, πληρότητα, συνέπεια και συνοχή των υποβαλλόμενων στοιχείων.

4. Η διαδικασία δεν περιλαμβάνει εργαστηριακές δοκιμές, δοκιμές διείσδυσης, έλεγχο πηγαίου κώδικα, επιτόπια τεχνική επαλήθευση ή άλλη ανεξάρτητη δοκιμή της πραγματικής λειτουργίας ή υλοποίησης του Τεχνολογικού Συστήματος.

5. Εκθέσεις δοκιμών, ελέγχων, πιστοποιήσεων ή τεχνικών αξιολογήσεων τρίτων μπορούν να λαμβάνονται υπόψη ως τεκμήρια, χωρίς να δεσμεύουν το ΚΕΜΕΑ και χωρίς αυτό να σημαίνει ότι το ΚΕΜΕΑ επαναλαμβάνει ή επιβεβαιώνει αυτοτελώς τις αντίστοιχες δοκιμές.

6. Η μη υποβολή επαρκούς τεκμηρίωσης δεν λογίζεται ως ύπαρξη του αντίστοιχου μέτρου ή μηχανισμού.

7. Το ΚΕΜΕΑ δύναται σε οποιοδήποτε στάδιο να ζητήσει πρόσθετες πληροφορίες, τεχνικές διευκρινίσεις ή συμπληρωματικά τεκμήρια.

8. Κατά την αξιολόγηση σταθμίζεται η αποδεικτική αξία κάθε τεκμηρίου ανάλογα με το είδος, την προέλευση, την επικαιρότητα και την αντιστοιχία του προς το Αντικείμενο Αξιολόγησης. Αφηγηματική περιγραφή ή δήλωση του αιτούντος, χωρίς υποστηρικτικό τεχνικό τεκμήριο, δεν αρκεί για βαθμολογία ίση ή ανώτερη των έξι μονάδων σε οποιοδήποτε κριτήριο. Όταν η Κατάσταση Συστήματος είναι «Υπό ανάπτυξη», ως τεχνικά τεκμήρια λογίζονται ιδίως τα αρχιτεκτονικά διαγράμματα, το μοντέλο απειλών, οι προδιαγραφές ασφάλειας και ο τεκμηριωμένος σχεδιασμός των μέτρων και μηχανισμών ασφάλειας.

Άρθρο 5

Αρχές της διαδικασίας και αρμόδια όργανα

1. Η διαδικασία διέπεται από τις αρχές της αντικειμενικότητας, της αμεροληψίας, της τεχνικής επάρκειας, της εμπιστευτικότητας, της ίσης μεταχείρισης, της τεκμηριωμένης λήψης αποφάσεων και της αποφυγής σύγκρουσης συμφερόντων.

2. Πρόσωπο που συμμετέχει στην αξιολόγηση δεν μπορεί να λαμβάνει ή να συμμετέχει στη λήψη της τελικής απόφασης πιστοποίησης του ίδιου Αντικειμένου Αξιολόγησης.

3. Με απόφαση του Διοικητικού Συμβουλίου του ΚΕΜΕΑ καθορίζονται τα όργανα και τα πρόσωπα που είναι υπεύθυνα για την εφαρμογή της παρούσας διαδικασίας, και ιδίως για:

α) τον ορισμό αξιολογητή ή ομάδας αξιολόγησης και επανεξεταστή,
β) την λήψη απόφασης πιστοποίησης,
γ) την κρίση επί μεταβολών, την καταχώριση εκδόσεων, τη μεταβολή της Κατάστασης Συστήματος και την ετήσια τεκμηριωτική επιτήρηση κατά τα άρθρα 28 και 29,
δ) την αναστολή, την αποκατάσταση και την ανάκληση πιστοποιητικού,
ε) την εξέταση ενστάσεων,
στ) την έγκριση του Οδηγού Βαθμολόγησης και των υποδειγμάτων της παρούσας,

4. Το ίδιο πρόσωπο ή όργανο μπορεί να διενεργεί την επανεξέταση και να λαμβάνει την απόφαση πιστοποίησης, όχι όμως ο αξιολογητής.

5. Δεν ορίζεται αξιολογητής ή επανεξεταστής πρόσωπο που συμμετείχε στον σχεδιασμό, την ανάπτυξη ή την παροχή συμβουλών ασφάλειας για το Αντικείμενο Αξιολόγησης κατά τα δύο τελευταία έτη πριν από την υποβολή της αίτησης ή έχει άλλη σχέση με τον αιτούντα ικανή να θέσει σε αμφιβολία την αμεροληψία του.

6. Τα πρόσωπα που συμμετέχουν στη διαδικασία, συμπεριλαμβανομένων εξωτερικών εμπειρογνωμόνων, υποβάλλουν δήλωση απουσίας σύγκρουσης συμφερόντων και δεσμεύονται εγγράφως για την τήρηση εμπιστευτικότητας. Η συνδρομή εξωτερικών εμπειρογνωμόνων δεν μεταβιβάζει την αρμοδιότητα λήψης απόφασης.

Άρθρο 6

Υποβολή αίτησης

1. Η διαδικασία αρχίζει με αίτηση προς το ΚΕΜΕΑ.

2. Η αίτηση περιλαμβάνει τουλάχιστον:

α) τα στοιχεία του αιτούντος,
β) την ονομασία του Συστήματος,
γ) τον κατασκευαστή, πάροχο ή υπεύθυνο ανάπτυξης, κατά περίπτωση,
δ) τον ακριβή προσδιορισμό της έκδοσης, διαμόρφωσης ή αρχιτεκτονικής που υποβάλλεται,
ε) συνοπτική περιγραφή του σκοπού και των βασικών λειτουργιών,
στ) τα όρια του Αντικειμένου Αξιολόγησης και τα στοιχεία που εξαιρούνται,
ζ) την κατάσταση του Συστήματος ως προς την υλοποίηση και την αντίστοιχη Κατάσταση Συστήματος κατά το άρθρο 3 παρ. 10.

3. Ο αιτών δηλώνει ότι τα στοιχεία που υποβάλλει είναι ακριβή, πλήρη και αντιστοιχούν στο Αντικείμενο Αξιολόγησης. Η δήλωση υποβάλλεται ως Υπεύθυνη Δήλωση του ν. 1599/1986 του αιτούντος ή του νόμιμου εκπροσώπου του ή, για αιτούντες εγκατεστημένους εκτός Ελλάδας, ως ισοδύναμη δήλωση κατά το δίκαιο της χώρας εγκατάστασής τους, και καλύπτει και τη δήλωση της περ. κζ΄ της παρ. 2 του άρθρου 8. Ο αιτών φέρει την αποκλειστική ευθύνη για την ακρίβεια και την πληρότητα των στοιχείων που υποβάλλει και για κάθε ζημία του ΚΕΜΕΑ ή τρίτων που οφείλεται σε ανακρίβεια ή απόκρυψη στοιχείων.

4. Με την υποβολή της αίτησης ο αιτών αποδέχεται τους όρους της παρούσας, συμπεριλαμβανομένων των όρων χρήσης της πιστοποίησης και της καταχώρισης στο Μητρώο του άρθρου 33.

5. Όταν ο αιτών δεν είναι ο κατασκευαστής ή ο πάροχος του Συστήματος, το Αντικείμενο Αξιολόγησης περιορίζεται στη συγκεκριμένη εγκατάσταση ή διαμόρφωση που χρησιμοποιεί, εγκαθιστά ή προσφέρει ο αιτών, εκτός αν ο κατασκευαστής ή ο πάροχος συναινεί εγγράφως ώστε η πιστοποίηση να αφορά συγκεκριμένη τυποποιημένη έκδοση και διαμόρφωση του Τεχνολογικού Συστήματος. Ο αιτών ευθύνεται ότι νομίμως διαθέτει τα στοιχεία που υποβάλλει.

6. Ο αιτών μπορεί να ανακαλέσει την αίτησή του σε κάθε στάδιο πριν από την έκδοση απόφασης.

Άρθρο 7

Αρχικός έλεγχος της αίτησης

1. Το ΚΕΜΕΑ εξετάζει αν:

α) το αντικείμενο εμπίπτει στο πεδίο της παρούσας,
β) το Αντικείμενο Αξιολόγησης προσδιορίζεται επαρκώς,
γ) υπάρχουν επαρκείς προϋποθέσεις για ουσιαστική τεχνική αξιολόγηση,
δ) διαθέτει ή μπορεί να εξασφαλίσει την αναγκαία τεχνική επάρκεια,
ε) δεν υφίσταται σύγκρουση συμφερόντων που εμποδίζει την αξιολόγηση.

2. Η αποδοχή της αίτησης δεν προδικάζει το αποτέλεσμα της πιστοποίησης.

3. Εάν δεν συντρέχουν οι προϋποθέσεις της παρ. 1, η αίτηση απορρίπτεται με αιτιολογημένη απόφαση, η οποία κοινοποιείται στον αιτούντα.

4. Το ΚΕΜΕΑ χορηγεί στον αιτούντα βεβαίωση με την ημερομηνία από την οποία υπολογίζεται ο χρόνος έκδοσης της απόφασης κατά το άρθρο 26 παρ. 5. Κατόπιν αιτήματος, χορηγεί βεβαίωση εκκρεμούς αίτησης, στην οποία αναφέρεται και τυχόν αναστολή του χρόνου αυτού.

Άρθρο 8

Τεχνικός Φάκελος Ασφάλειας

1. Ο αιτών υποβάλλει Τεχνικό Φάκελο Ασφάλειας ανάλογο με τη φύση του Αντικειμένου Αξιολόγησης.

2. Ο φάκελος περιλαμβάνει, κατά περίπτωση:

α) αναλυτική περιγραφή του Συστήματος,
β) αρχιτεκτονική Συστήματος,
γ) διαγράμματα υποσυστημάτων και διασυνδέσεων,
δ) διαγράμματα ροής δεδομένων,
ε) όρια εμπιστοσύνης,
στ) εξωτερικές και εσωτερικές διεπαφές,
ζ) πρωτόκολλα επικοινωνίας και εκδόσεις τους,
η) μηχανισμούς κρυπτογράφησης,
θ) μεθόδους και παραμέτρους διαχείρισης κλειδιών,
ι) μηχανισμούς ταυτοποίησης και αυθεντικοποίησης,
ια) διαχείριση ρόλων και δικαιωμάτων,
ιβ) στοιχεία για προνομιακούς λογαριασμούς,
ιγ) θύρες, υπηρεσίες και σημεία δικτυακής έκθεσης,
ιδ) APIs και λοιπές τεχνικές διεπαφές,
ιε) προστασία δεδομένων κατά τη μεταφορά και αποθήκευση,
ιστ) μηχανισμούς καταγραφής και παρακολούθησης,
ιζ) μηχανισμούς ασφαλούς διαμόρφωσης,
ιη) διαδικασία διαχείρισης ευπαθειών,
ιθ) διαδικασία ενημερώσεων και διορθώσεων,
κ) προβλέψεις διαθεσιμότητας και ανάκτησης,
κα) εξαρτήσεις και συστατικά τρίτων,
κβ) στοιχεία για υλικολογισμικό και κρίσιμα στοιχεία υλικού, όπου εφαρμόζονται,
κγ) στοιχεία για τη διαδικασία ανάπτυξης και διάθεσης εκδόσεων,
κδ) εκθέσεις δοκιμών ασφάλειας και προηγούμενες εκθέσεις ελέγχων ή πιστοποιήσεων,
κε) μοντέλο απειλών ή ανάλυση κινδύνων,
κστ) παραδοχές για το περιβάλλον λειτουργίας και κατανομή των ευθυνών ασφάλειας μεταξύ κατασκευαστή, παρόχου και χρήστη,
κζ) δήλωση γνωστών μη αντιμετωπισμένων ευπαθειών και ανοικτών ευρημάτων ελέγχων που αφορούν το Αντικείμενο Αξιολόγησης, καθώς και του τρόπου αντιμετώπισής τους,
κη) στοιχεία φυσικής προστασίας του υλικού εξοπλισμού, όπου εφαρμόζεται,
κθ) οδηγίες ασφαλούς εγκατάστασης και διαμόρφωσης προς τον χρήστη,
λ) κάθε άλλο στοιχείο που ζητεί το ΚΕΜΕΑ.

3. Το ΚΕΜΕΑ δύναται να καθορίζει υποδείγματα ή ειδικότερες απαιτήσεις για την υποβολή του Τεχνικού Φακέλου Ασφάλειας.

4. Ο Τεχνικός Φάκελος Ασφάλειας υποβάλλεται στην ελληνική ή την αγγλική γλώσσα, με ασφαλή τρόπο που ορίζει το ΚΕΜΕΑ.

Άρθρο 9

Πλαίσια αναφοράς και φύση της πιστοποίησης

1. Για την αξιολόγηση και την επικαιροποίηση της μεθοδολογίας το ΚΕΜΕΑ δύναται να λαμβάνει υπόψη διεθνή, ευρωπαϊκά και εθνικά πρότυπα, κατευθυντήριες οδηγίες και αναγνωρισμένες τεχνικές πρακτικές ασφάλειας.

2. Η χρήση τέτοιων πηγών δεν συνεπάγεται ότι η πιστοποίηση αποτελεί πιστοποίηση συμμόρφωσης προς συγκεκριμένο πρότυπο.

3. Η πιστοποίηση κατά την παρούσα είναι προαιρετική και δεν αποτελεί:

α) ευρωπαϊκό ή εθνικό σχήμα πιστοποίησης της κυβερνοασφάλειας ούτε πιστοποιητικό κυβερνοασφάλειας κατά τον Κανονισμό (ΕΕ) 2019/881 (Cybersecurity Act) και δεν εκδίδεται στο πλαίσιο αυτού,
β) διαδικασία αξιολόγησης συμμόρφωσης για τους σκοπούς σήμανσης CE ή άλλης ειδικής ενωσιακής ή εθνικής νομοθεσίας και δεν παρέχει τεκμήριο συμμόρφωσης προς απαιτήσεις τέτοιας νομοθεσίας,
γ) διαπιστευμένη πιστοποίηση κατά τον Κανονισμό (ΕΚ) 765/2008,
δ) πιστοποίηση κατά το άρθρο 42 του Κανονισμού (ΕΕ) 2016/679.

Άρθρο 10

Σύστημα βαθμολόγησης

1. Κάθε Αντικείμενο Αξιολόγησης αξιολογείται βάσει δέκα Κριτηρίων Ασφάλειας.

2. Κάθε κριτήριο βαθμολογείται αυτοτελώς από μηδέν έως δέκα μονάδες.

3. Η συνολική Βαθμολογία Ασφάλειας προκύπτει από το απλό άθροισμα των δέκα βαθμολογιών και κυμαίνεται από μηδέν έως εκατό.

4. Δεν εφαρμόζονται συντελεστές βαρύτητας, ποσοστιαίες αναγωγές ή διαφορετικές κλίμακες.

5. Τα ίδια δέκα κριτήρια εφαρμόζονται σε συστήματα λογισμικού, υλικού εξοπλισμού και μικτά συστήματα.

6. Κάθε ιδιότητα, μέτρο ή μηχανισμός ασφάλειας βαθμολογείται μία μόνο φορά.

7. Δεν επιτρέπεται η διπλή προσμέτρηση του ίδιου χαρακτηριστικού σε περισσότερα κριτήρια.

8. Τα επιμέρους στοιχεία κάθε κριτηρίου εφαρμόζονται στο μέτρο που αρμόζουν στη φύση, την Κατάσταση Συστήματος και τα όρια του Αντικειμένου Αξιολόγησης. Στοιχεία που δεν εφαρμόζονται δεν λαμβάνονται υπόψη και η μη εφαρμογή τους αιτιολογείται στην Έκθεση Αξιολόγησης. Κατά κανόνα κανένα κριτήριο δεν κρίνεται μη εφαρμοστέο στο σύνολό του. Κατ' εξαίρεση, εφόσον μετά από ειδικά αιτιολογημένη εξέταση εφαρμοσιμότητας διαπιστώνεται ότι κανένα επιμέρους στοιχείο συγκεκριμένου Κριτηρίου Ασφάλειας δεν είναι εφαρμοστέο στο Αντικείμενο Αξιολόγησης λόγω της φύσης και της τεκμηριωμένης αρχιτεκτονικής του, το κριτήριο βαθμολογείται με έξι (6) μονάδες αποκλειστικά για τη διατήρηση της ενιαίας κλίμακας βαθμολόγησης. Η βαθμολογία αυτή δεν συνιστά θετική αξιολόγηση μέτρων ασφάλειας ούτε επιβράβευση της μη εφαρμογής. Η πλήρης μη εφαρμογή του κριτηρίου αιτιολογείται ειδικά στην Έκθεση Αξιολόγησης και επιβεβαιώνεται κατά την ανεξάρτητη επανεξέταση του άρθρου 25. Όταν η Κατάσταση Συστήματος είναι «Υπό ανάπτυξη», σε κάθε κριτήριο αξιολογούνται τα μέτρα και οι μηχανισμοί που προβλέπει η τεκμηριωμένη αρχιτεκτονική και ο σχεδιασμός.

9. Όταν ένα χαρακτηριστικό μπορεί να υπαχθεί σε περισσότερα κριτήρια, βαθμολογείται μόνο στο κριτήριο που ορίζει ο Οδηγός Βαθμολόγησης ή, ελλείψει πρόβλεψης, στο ειδικότερο κριτήριο. Η υπαγωγή σημειώνεται στην Έκθεση Αξιολόγησης.

10. Η εφαρμογή των κριτηρίων εξειδικεύεται σε Οδηγό Βαθμολόγησης, ο οποίος περιλαμβάνει ιδίως την κατανομή χαρακτηριστικών μεταξύ των κριτηρίων, παραδείγματα ανά επίπεδο βαθμολογίας και τύπο συστήματος, την αποδεικτική αξία των κατηγοριών τεκμηρίων και παραδείγματα Κρίσιμων Αδυναμιών. Ο Οδηγός εγκρίνεται κατά το άρθρο 5 παρ. 3, φέρει αριθμό έκδοσης και οι τροποποιήσεις του δεν εφαρμόζονται σε εκκρεμείς αιτήσεις. Ο Οδηγός Βαθμολόγησης δημοσιεύεται στον διαδικτυακό τόπο του ΚΕΜΕΑ.

Άρθρο 11

Γενική κλίμακα βαθμολόγησης

Η ακόλουθη κλίμακα χρησιμοποιείται σε όλα τα κριτήρια και εφαρμόζεται επί του επιπέδου που προκύπτει από την Τεκμηριωτική Αξιολόγηση Ασφάλειας:

0: Το αντικείμενο του κριτηρίου δεν καλύπτεται, εφαρμόζεται κατά μη ασφαλή τρόπο ή δεν έχει προσκομισθεί επαρκής τεκμηρίωση.

2: Υπάρχει στοιχειώδης κάλυψη, αλλά διαπιστώνονται σοβαρές ελλείψεις.

4: Υπάρχει ουσιαστική αλλά μερική κάλυψη, με σημαντικά περιθώρια βελτίωσης.

6: Το κριτήριο καλύπτεται σε ικανοποιητικό επίπεδο χωρίς σοβαρές αδυναμίες.

8: Το κριτήριο καλύπτεται σε υψηλό επίπεδο με σύγχρονα, συνεκτικά και επαρκώς τεκμηριωμένα μέτρα.

10: Το κριτήριο καλύπτεται πλήρως ή σχεδόν πλήρως με ισχυρούς, σύγχρονους και αναλυτικά τεκμηριωμένους μηχανισμούς ασφάλειας.

Οι βαθμοί 1, 3, 5, 7 και 9 χρησιμοποιούνται όταν η αξιολόγηση βρίσκεται μεταξύ δύο διαδοχικών επιπέδων.

Δεν χρησιμοποιούνται δεκαδικοί βαθμοί.

Κατ' εξαίρεση, η βαθμολογία έξι (6) μονάδων που προβλέπεται στο άρθρο 10 παρ. 8 για πλήρως μη εφαρμοστέο κριτήριο έχει ουδέτερο τεχνικό χαρακτήρα και δεν ερμηνεύεται ως θετική αξιολόγηση μέτρων ασφάλειας.

Άρθρο 12

Κριτήριο 1: Αρχιτεκτονική Ασφάλειας και Μοντέλο Απειλών

Βαθμολογία: 0 έως 10.

Αξιολογούνται ιδίως:

α) η σαφής αποτύπωση της αρχιτεκτονικής,
β) τα βασικά συστατικά,
γ) οι ροές δεδομένων,
δ) τα όρια εμπιστοσύνης,
ε) οι επιφάνειες επίθεσης,

στ) οι βασικές απειλές,
ζ) οι σχεδιαστικές αρχές ασφάλειας,
η) η συνοχή μεταξύ κινδύνων και αρχιτεκτονικών μέτρων,
θ) οι παραδοχές για το περιβάλλον λειτουργίας και τα όρια του Αντικειμένου Αξιολόγησης.

Στο παρόν κριτήριο δεν επαναβαθμολογούνται συγκεκριμένοι μηχανισμοί που αξιολογούνται στα επόμενα κριτήρια. Αξιολογείται η ποιότητα και η πληρότητα της ανάλυσης και όχι η ισχύς των επιμέρους μέτρων.

Άρθρο 13

Κριτήριο 2: Ταυτοποίηση, Αυθεντικοποίηση και Έλεγχος Πρόσβασης

Βαθμολογία: 0 έως 10.

Αξιολογούνται ιδίως:

α) η διαχείριση ταυτοτήτων,
β) οι μηχανισμοί αυθεντικοποίησης,
γ) η πολυπαραγοντική αυθεντικοποίηση όπου απαιτείται,
δ) οι ρόλοι, τα δικαιώματα και οι αποφάσεις εξουσιοδότησης σε επίπεδο λειτουργίας και δεδομένων,
ε) η αρχή του ελάχιστου αναγκαίου δικαιώματος,
στ) οι προνομιακοί και προεπιλεγμένοι λογαριασμοί και διαπιστευτήρια,
ζ) ο κύκλος ζωής λογαριασμών και δικαιωμάτων,
η) οι ταυτότητες συσκευών και υπηρεσιών,
θ) η έκδοση, λήξη και ανάκληση συνεδριών.

Η κρυπτογραφική ισχύς και η προστασία διαπιστευτηρίων και tokens αξιολογούνται στο Κριτήριο 3.

Άρθρο 14

Κριτήριο 3: Προστασία Δεδομένων και Κρυπτογραφία

Βαθμολογία: 0 έως 10.

Αξιολογούνται ιδίως:

α) η προστασία δεδομένων κατά τη μεταφορά,
β) η προστασία δεδομένων κατά την αποθήκευση,
γ) οι αλγόριθμοι και τα κρυπτογραφικά πρωτόκολλα,
δ) οι εκδόσεις κρυπτογραφικών πρωτοκόλλων,
ε) τα μήκη και οι παράμετροι κλειδιών,
στ) η δημιουργία, αποθήκευση, ανανέωση και ανάκληση κλειδιών, συμπεριλαμβανομένων των κλειδιών υπογραφής κώδικα και υλικολογισμικού,
ζ) η προστασία διαπιστευτηρίων, tokens, certificates και λοιπών μυστικών,
η) η ασφαλής παύση χρήσης ή διαγραφή ευαίσθητων στοιχείων,

θ) η κρυπτογραφική προστασία της ακεραιότητας δεδομένων,
ι) η δυνατότητα αντικατάστασης κρυπτογραφικών αλγορίθμων.

Ο όρος «προστασία δεδομένων» στο παρόν κριτήριο αφορά την ασφάλεια των δεδομένων, συμπεριλαμβανομένων και των δεδομένων προσωπικού χαρακτήρα, αλλά όχι τη νομιμότητα της επεξεργασίας τους. Η ποιότητα της κρυπτογραφίας και της διαχείρισης κλειδιών αξιολογείται αποκλειστικά στο παρόν κριτήριο, όπου κι αν αυτή χρησιμοποιείται.

Άρθρο 15

Κριτήριο 4: Ασφάλεια Επικοινωνιών, Δικτύων και Διεπαφών

Βαθμολογία: 0 έως 10.

Αξιολογούνται ιδίως:

α) οι ενεργές υπηρεσίες και θύρες,
β) η δικτυακή έκθεση,
γ) η τμηματοποίηση και ο διαχωρισμός,
δ) οι διεπαφές διαχείρισης,
ε) τα APIs ως σημεία έκθεσης,
στ) οι επικοινωνίες μεταξύ ζωνών εμπιστοσύνης,
ζ) η απομακρυσμένη διαχείριση,
η) η απενεργοποίηση μη αναγκαίων επικοινωνιακών λειτουργιών,
θ) οι ασύρματες διεπαφές, όπου υπάρχουν.

Η ποιότητα της κρυπτογραφικής προστασίας αξιολογείται αποκλειστικά στο Κριτήριο 3. Η προστασία από άρνηση υπηρεσίας αξιολογείται στο Κριτήριο 8.

Άρθρο 16

Κριτήριο 5: Ακεραιότητα Συστήματος, Εκτέλεσης και Λειτουργιών

Βαθμολογία: 0 έως 10.

Αξιολογούνται, ανάλογα με τη φύση του Συστήματος:

α) η ασφαλής επεξεργασία μη έμπιστων εισόδων,
β) η προστασία από μη επιτρεπτή μεταβολή της προβλεπόμενης εκτέλεσης,
γ) η ακεραιότητα επιχειρησιακών ροών,
δ) η προστασία συνεδριών και κατάστασης εφαρμογής,
ε) η απομόνωση διεργασιών, χρηστών, tenants ή κρίσιμων λειτουργιών,
στ) η ασφαλής εκκίνηση,
ζ) η ακεραιότητα firmware,
η) η χρήση μηχανισμών ασφάλειας βασισμένων σε υλικό (π.χ. TPM, secure element) όπου εφαρμόζεται,
θ) η προστασία φυσικών διεπαφών και διεπαφών αποσφαλμάτωσης (π.χ. JTAG, UART, θύρες service),

ι) η συνέχεια της αλυσίδας εμπιστοσύνης εκκίνησης και εκτέλεσης σε μικτά συστήματα,
ια) η προστασία από φυσική παραβίαση και η ανίχνευσή της, όπου εφαρμόζεται.

Στο παρόν κριτήριο αξιολογείται η επαλήθευση της ακεραιότητας κατά την εκκίνηση και την εκτέλεση. Η επαλήθευση ενημερώσεων πριν από την εγκατάσταση αξιολογείται στο Κριτήριο 7, η ακεραιότητα κατά την παραγωγή εκδόσεων στο Κριτήριο 10 και η συμπεριφορά σε περίπτωση αστοχίας στο Κριτήριο 8.

Άρθρο 17

Κριτήριο 6: Καταγραφή, Ιχνηλασιμότητα και Παρακολούθηση

Βαθμολογία: 0 έως 10.

Αξιολογούνται ιδίως:

α) η καταγραφή κρίσιμων ενεργειών,
β) η καταγραφή ενεργειών διαχειριστών,
γ) η καταγραφή αποτυχημένων ή ύποπτων προσπαθειών,
δ) η απόδοση ενεργειών σε συγκεκριμένη ταυτότητα,
ε) η προστασία των αρχείων καταγραφής,
στ) η χρονική συνέπεια των καταγραφών,
ζ) η διάρκεια διατήρησης,
η) η δυνατότητα παρακολούθησης και παραγωγής ειδοποιήσεων,
θ) η δυνατότητα υποστήριξης διερεύνησης περιστατικών,
ι) η δυνατότητα εξαγωγής των καταγραφών σε εξωτερικά συστήματα παρακολούθησης.

Άρθρο 18

Κριτήριο 7: Διαχείριση Ευπαθειών, Διαμόρφωσης και Ενημερώσεων

Βαθμολογία: 0 έως 10.

Αξιολογούνται ιδίως:

α) η ύπαρξη και τήρηση τεκμηριωμένης ασφαλούς βασικής διαμόρφωσης, χωρίς επαναβαθμολόγηση επιμέρους ρυθμίσεων που αξιολογούνται σε άλλα κριτήρια,
β) η διαχείριση προεπιλεγμένων ρυθμίσεων,
γ) η απενεργοποίηση περιττών λειτουργιών πλην των επικοινωνιακών,
δ) η παρακολούθηση γνωστών ευπαθειών, συμπεριλαμβανομένων των ευπαθειών τρίτων συστατικών,
ε) η αντιμετώπιση ευπαθειών,
στ) η διάθεση και εφαρμογή διορθώσεων,
ζ) η ασφαλής ενημέρωση,
η) η προστασία από μη εξουσιοδοτημένη ενημέρωση και η επαλήθευση της ακεραιότητας των ενημερώσεων πριν από την εγκατάσταση,
θ) η περίοδος υποστήριξης του Αντικειμένου Αξιολόγησης,

ι) η αντιμετώπιση λήξης υποστήριξης,
ια) η πολιτική συντονισμένης γνωστοποίησης ευπαθειών και ο δίαυλος υποβολής αναφορών,
ιβ) η ενημέρωση των χρηστών για ευπάθειες και διορθώσεις.

Άρθρο 19

Κριτήριο 8: Διαθεσιμότητα, Ανθεκτικότητα και Ανάκτηση

Βαθμολογία: 0 έως 10.

Αξιολογούνται ιδίως:

α) τα μοναδικά σημεία αστοχίας,
β) η εφεδρεία όπου απαιτείται,
γ) η προστασία από εξάντληση πόρων, συμπεριλαμβανομένης της άρνησης υπηρεσίας,
δ) τα αντίγραφα ασφαλείας και η προστασία τους από κακόβουλη διαγραφή ή αλλοίωση,
ε) η ανάκτηση δεδομένων και η δοκιμή της,
στ) η αποκατάσταση λειτουργίας,
ζ) η συμπεριφορά σε περίπτωση μερικής αστοχίας,
η) η δυνατότητα ασφαλούς υποβάθμισης λειτουργίας,
θ) η αποφυγή μετάπτωσης σε μη ασφαλή κατάσταση.

Στο παρόν κριτήριο αξιολογούνται και οι συνέπειες της μη διαθεσιμότητας εξωτερικών παρόχων για τη λειτουργία του Συστήματος.

Άρθρο 20

Κριτήριο 9: Εξαρτήσεις, Τρίτα Συστατικά και Αλυσίδα Εφοδιασμού

Βαθμολογία: 0 έως 10.

Αξιολογούνται ιδίως:

α) η καταγραφή κρίσιμων τρίτων συστατικών,
β) οι εκδόσεις τους,
γ) η κατάσταση υποστήριξής τους,
δ) η προέλευσή τους,
ε) η επαλήθευση της ακεραιότητας και γνησιότητας των εισερχόμενων συστατικών λογισμικού και υλικού,
στ) οι εξωτερικές υπηρεσίες και APIs,
ζ) οι εξαρτήσεις από παρόχους,
η) η δυνατότητα αντικατάστασης προβληματικού συστατικού,
θ) η ύπαρξη κατάλληλου καταλόγου συστατικών όπου εφαρμόζεται.

Στο παρόν κριτήριο αξιολογούνται αποκλειστικά ζητήματα που αφορούν συστατικά, υπηρεσίες και παρόχους τρίτων. Οι ιδιότητες ασφάλειας που υλοποιούνται μέσω αυτών βαθμολογούνται στο οικείο κριτήριο και η διαχείριση των ευπαθειών τους στο Κριτήριο 7.

Άρθρο 21

Κριτήριο 10: Ασφαλής Ανάπτυξη, Μεταβολές και Διάθεση Εκδόσεων

Βαθμολογία: 0 έως 10.

Αξιολογούνται ιδίως:

α) οι απαιτήσεις ασφάλειας κατά τον σχεδιασμό,
β) οι κανόνες ασφαλούς ανάπτυξης ή κατασκευής,
γ) η διαχείριση τεχνικών μεταβολών, συμπεριλαμβανομένων των μεταβολών διαμόρφωσης σε παραγωγική λειτουργία,
δ) ο έλεγχος αλλαγών κώδικα, firmware ή σχεδιασμού,
ε) ο διαχωρισμός περιβαλλόντων,
στ) η προστασία της διαδικασίας build ή παραγωγής,
ζ) η ιχνηλασιμότητα εκδόσεων,
η) η ακεραιότητα και η υπογραφή των παραγόμενων εκδόσεων κατά την παραγωγή τους,
θ) η διαδικασία διάθεσης νέων εκδόσεων,
ι) η ενσωμάτωση της ασφάλειας στον κύκλο ζωής ανάπτυξης,
ια) οι δοκιμές ασφάλειας κατά την ανάπτυξη (π.χ. στατική και δυναμική ανάλυση, fuzzing, δοκιμές διείσδυσης) και η διαχείριση των ευρημάτων τους.

Στο παρόν κριτήριο αξιολογείται η διαδικασία ανάπτυξης και όχι το περιεχόμενο του μοντέλου απειλών, που αξιολογείται στο Κριτήριο 1. Η έγκαιρη διάθεση διορθώσεων ασφάλειας αξιολογείται στο Κριτήριο 7.

Άρθρο 22

Κρίσιμες Αδυναμίες

1. Ως Κρίσιμη Αδυναμία νοείται η αδυναμία που ορίζεται στην παρ. 7 του άρθρου 3.

2. Ενδεικτικά μπορούν να αποτελούν Κρίσιμες Αδυναμίες:

α) μη αυθεντικοποιημένη πρόσβαση σε κρίσιμη ή προνομιακή λειτουργία,
β) κοινά και μη μεταβαλλόμενα προνομιακά διαπιστευτήρια,
γ) μετάδοση κρίσιμων διαπιστευτηρίων ή ιδιαίτερα ευαίσθητων δεδομένων χωρίς κατάλληλη προστασία μέσω μη έμπιστου δικτύου,
δ) χρήση αποδεδειγμένα μη ασφαλούς κρυπτογραφικού μηχανισμού σε κρίσιμη λειτουργία,
ε) δυνατότητα εγκατάστασης μη εξουσιοδοτημένου κώδικα ή firmware σε κρίσιμο στοιχείο,
στ) δυνατότητα μη εξουσιοδοτημένης πρόσβασης σε δεδομένα άλλου χρήστη ή tenant λόγω ανεπαρκούς απομόνωσης,
ζ) γνωστή και μη αντιμετωπισμένη ευπάθεια σε κρίσιμο στοιχείο, για την οποία υπάρχουν ενδείξεις ενεργής εκμετάλλευσης,
η) κρίσιμο στοιχείο εκτός υποστήριξης ασφάλειας, χωρίς επαρκή αντισταθμιστικά μέτρα,
θ) άλλη αδυναμία αντίστοιχης σοβαρότητας.

3. Ο χαρακτηρισμός μιας αδυναμίας ως κρίσιμης αιτιολογείται ειδικά στην Έκθεση Αξιολόγησης.

4. Η Κρίσιμη Αδυναμία αποτελεί αυτοτελές κριτήριο αποκλεισμού και δεν επιφέρει πρόσθετη αριθμητική αφαίρεση.

5. Ανοικτό εύρημα κρίσιμης σοβαρότητας σε έκθεση τρίτου που αφορά το Αντικείμενο Αξιολόγησης θεωρείται Κρίσιμη Αδυναμία, εκτός αν τεκμηριωθεί η αντιμετώπισή του.

Άρθρο 23

Έκθεση Αξιολόγησης

1. Για κάθε Αντικείμενο Αξιολόγησης συντάσσεται Έκθεση Αξιολόγησης.

2. Η Έκθεση περιλαμβάνει τουλάχιστον:

α) τα στοιχεία του Αντικειμένου Αξιολόγησης,
β) την έκδοση, διαμόρφωση ή αρχιτεκτονική που αξιολογήθηκε, τα όρια του Αντικειμένου Αξιολόγησης, τα στοιχεία που εξαιρούνται, τις παραδοχές περιβάλλοντος λειτουργίας και την Κατάσταση Συστήματος,
γ) τα βασικά τεκμήρια που εξετάστηκαν,
δ) βαθμολογία από μηδέν έως δέκα για καθένα από τα δέκα κριτήρια,
ε) συνοπτική αιτιολόγηση κάθε βαθμολογίας, με διάκριση αν χαμηλή βαθμολογία οφείλεται σε έλλειψη τεκμηρίωσης ή σε αδυναμία που προκύπτει από τα τεκμήρια,
στ) τη συνολική Βαθμολογία Ασφάλειας,
ζ) τις κύριες αδυναμίες και περιορισμούς,
η) τυχόν Κρίσιμες Αδυναμίες,
θ) το τελικό συμπέρασμα.

3. Η βαθμολογία βασίζεται αποκλειστικά στα στοιχεία που τέθηκαν υπόψη του ΚΕΜΕΑ.

4. Η Έκθεση Αξιολόγησης κοινοποιείται στον αιτούντα μαζί με την απόφαση.

Άρθρο 24

Συμπληρωματικά στοιχεία

1. Πριν από την οριστικοποίηση της αξιολόγησης, το ΚΕΜΕΑ δύναται να ζητήσει πρόσθετα στοιχεία ή διευκρινίσεις.

2. Ο αιτών δύναται να υποβάλει συμπληρωματική τεκμηρίωση ή στοιχεία σχετικά με μεταβολές που πραγματοποίησε στο Σύστημα. Εάν οι μεταβολές αφορούν το Αντικείμενο Αξιολόγησης, ο αιτών επικαιροποιεί τον προσδιορισμό της έκδοσης, διαμόρφωσης ή αρχιτεκτονικής κατά την περ. δ΄ της παρ. 2 του άρθρου 6.

3. Νέα στοιχεία λαμβάνονται υπόψη μόνο εφόσον υποβληθούν πριν από την ολοκλήρωση της αξιολόγησης ή στο πλαίσιο νέας αίτησης ή συμπληρωματικής αξιολόγησης.

4. Το ΚΕΜΕΑ τάσσει εύλογη προθεσμία για την υποβολή συμπληρωματικών στοιχείων. Αν η προθεσμία παρέλθει άπρακτη, η αξιολόγηση ολοκληρώνεται με βάση τα υπάρχοντα στοιχεία ή, αν αυτά δεν επαρκούν για ουσιαστική αξιολόγηση, η αίτηση αρχειοθετείται.

Άρθρο 25

Ανεξάρτητη επανεξέταση

1. Μετά την ολοκλήρωση της αξιολόγησης, ο φάκελος υποβάλλεται σε ανεξάρτητη επανεξέταση.

2. Η επανεξέταση πραγματοποιείται από πρόσωπο που δεν διενήργησε την αρχική αξιολόγηση.

3. Εξετάζονται ιδίως:

α) η πληρότητα του φακέλου,
β) η συνέπεια της βαθμολόγησης,
γ) η επάρκεια της αιτιολόγησης,
δ) η ορθή εφαρμογή της παρούσας,
ε) η τεκμηρίωση τυχόν Κρίσιμης Αδυναμίας.

4. Ο επανεξεταστής μπορεί να επιστρέψει τον φάκελο στον αξιολογητή με αιτιολογημένες παρατηρήσεις. Διαφωνία που παραμένει επιλύεται από το όργανο που λαμβάνει την απόφαση πιστοποίησης, το οποίο αιτιολογεί την κρίση του.

Άρθρο 26

Απόφαση πιστοποίησης

1. Η τελική απόφαση λαμβάνεται από αρμόδιο πρόσωπο ή όργανο, οριζόμενο κατά το άρθρο 5 παρ. 3, που δεν συμμετείχε στην αρχική αξιολόγηση.

2. Πιστοποιητικό χορηγείται εφόσον:

α) η συνολική Βαθμολογία Ασφάλειας είναι τουλάχιστον εβδομήντα μονάδες στις εκατό,
β) δεν έχει διαπιστωθεί Κρίσιμη Αδυναμία, και
γ) κανένα κριτήριο δεν έχει βαθμολογηθεί κάτω από έξι μονάδες.

3. Συνολική βαθμολογία εβδομήντα ή περισσότερων μονάδων δεν θεραπεύει την ύπαρξη Κρίσιμης Αδυναμίας.

4. Σε περίπτωση μη χορήγησης πιστοποιητικού, ο αιτών ενημερώνεται για το αποτέλεσμα και τους ουσιώδεις λόγους της απόφασης, καθώς και για τη δυνατότητα άσκησης ένστασης κατά το άρθρο 31.

5. Ο ελάχιστος και ο μέγιστος χρόνος έκδοσης της απόφασης αναφέρονται στην προσφορά του άρθρου 35 και υπολογίζονται από την ημερομηνία κατά την οποία ο Τεχνικός Φάκελος Ασφάλειας είναι πλήρης, χωρίς να απαιτούνται συμπληρώσεις, και έχει καταβληθεί η αμοιβή. Εάν στη συνέχεια διαπιστωθούν ελλείψεις ή ζητηθούν διευκρινίσεις ή συμπληρωματικά στοιχεία, ο χρόνος αναστέλλεται από την κοινοποίηση του σχετικού αιτήματος έως την πλήρη ανταπόκριση του αιτούντος.

Άρθρο 27

Πιστοποιητικό Τεκμηριωτικής Αξιολόγησης Ασφάλειας Τεχνολογικού Συστήματος ΚΕΜΕΑ

1. Σε περίπτωση θετικής απόφασης εκδίδεται Πιστοποιητικό Τεκμηριωτικής Αξιολόγησης Ασφάλειας Τεχνολογικού Συστήματος ΚΕΜΕΑ.

2. Το Πιστοποιητικό περιλαμβάνει τουλάχιστον:

α) μοναδικό αριθμό,
β) τον κάτοχο του πιστοποιητικού,
γ) την ονομασία του Συστήματος,
δ) τον ακριβή προσδιορισμό της έκδοσης, διαμόρφωσης ή αρχιτεκτονικής,
ε) τα όρια του Αντικειμένου Αξιολόγησης, τα στοιχεία που εξαιρούνται και την Κατάσταση Συστήματος,
στ) τη συνολική Βαθμολογία Ασφάλειας και, σε παράρτημα, τη βαθμολογία σε καθένα από τα δέκα κριτήρια,
ζ) την ημερομηνία έκδοσης,
η) την ημερομηνία λήξης,
θ) τυχόν περιορισμούς και τις ουσιώδεις παραδοχές περιβάλλοντος λειτουργίας,
ι) αναφορά ότι η αξιολόγηση πραγματοποιήθηκε βάσει της τεχνικής τεκμηρίωσης που τέθηκε υπόψη του ΚΕΜΕΑ,
ια) κωδικό ηλεκτρονικής επαλήθευσης, από τη θέση σε λειτουργία της εφαρμογής του άρθρου 33 παρ. 3.

3. Στο Πιστοποιητικό αναγράφεται ότι η αξιολόγηση δεν περιλαμβάνει εργαστηριακή δοκιμή, δοκιμή διείσδυσης, έλεγχο πηγαίου κώδικα ή ανεξάρτητη τεχνική επαλήθευση της πραγματικής υλοποίησης. Αναγράφεται επίσης ότι η πιστοποίηση δεν αποτελεί πιστοποιητικό κυβερνοασφάλειας κατά τον Κανονισμό (ΕΕ) 2019/881 (Cybersecurity Act), σήμανση CE ή διαπιστευμένη πιστοποίηση. Όταν η Κατάσταση Συστήματος είναι «Υπό ανάπτυξη», αναγράφεται ρητά ότι η πιστοποίηση αφορά την τεκμηριωμένη αρχιτεκτονική και τα προβλεπόμενα μέτρα και μηχανισμούς ασφάλειας και ότι η μεταβολή της Κατάστασης Συστήματος σε «Υλοποιημένο» προϋποθέτει τη συμπληρωματική τεκμηριωτική αξιολόγηση του άρθρου 28 παρ. 6.

4. Η πιστοποίηση δεν συνιστά εγγύηση ότι το Σύστημα είναι απαλλαγμένο από ευπάθειες ή ότι είναι αδύνατη η παραβίασή του.

Άρθρο 28

Διάρκεια ισχύος, Κατάσταση Συστήματος και επιτήρηση

1. Η διάρκεια ισχύος του πιστοποιητικού καθορίζεται στο ίδιο το πιστοποιητικό και δεν μπορεί να υπερβαίνει τα δύο έτη από την ημερομηνία έκδοσής του.

2. Με την επιφύλαξη των παρ. 4 έως 7 και του άρθρου 29 παρ. 5, η ισχύς αφορά αποκλειστικά την έκδοση, διαμόρφωση ή αρχιτεκτονική που αξιολογήθηκε.

3. Η παρέλευση της ημερομηνίας λήξης συνεπάγεται αυτοδικαίως παύση της ισχύος του πιστοποιητικού.

4. Η ισχύς μπορεί να καταλαμβάνει και μεταγενέστερες εκδόσεις που περιέχουν μόνο διορθώσεις ευπαθειών ή άλλες μεταβολές που δεν συνιστούν Ουσιώδεις Μεταβολές, εφόσον ο κάτοχος τις γνωστοποιεί στο ΚΕΜΕΑ εντός τριάντα ημερών από τη διάθεσή τους και προσκομίζει τα αναγκαία τεχνικά στοιχεία. Η καταχώριση της νέας έκδοσης στο Μητρώο δεν είναι αυτοδίκαιη και πραγματοποιείται μόνο μετά από έγγραφη τεχνική κρίση του ΚΕΜΕΑ ότι οι μεταβολές δεν επηρεάζουν ουσιωδώς τη Βαθμολογία Ασφάλειας, δεν δημιουργούν Κρίσιμη Αδυναμία και δεν μεταβάλλουν ουσιωδώς τις παραδοχές ή τα όρια του Αντικειμένου Αξιολόγησης. Το ΚΕΜΕΑ μπορεί να ζητήσει συμπληρωματική αξιολόγηση κατά το άρθρο 29 παρ. 5.

5. Όταν η αξιολόγηση αφορά σχεδιασμό, τεχνολογική αρχιτεκτονική ή Σύστημα του οποίου η υλοποίηση δεν έχει ολοκληρωθεί, στο Πιστοποιητικό και στο Μητρώο αναγράφεται Κατάσταση Συστήματος «Υπό ανάπτυξη». Με την ολοκλήρωση της υλοποίησης, ο κάτοχος ενημερώνει το ΚΕΜΕΑ και υποβάλλει τα τεχνικά στοιχεία της υλοποιημένης έκδοσης που απαιτούνται για τη συμπληρωματική τεκμηριωτική αξιολόγηση της παρ. 6.

6. Η συμπληρωματική τεκμηριωτική αξιολόγηση για τη μεταβολή της Κατάστασης Συστήματος σε «Υλοποιημένο» εξετάζει, βάσει των προσκομιζόμενων στοιχείων, αν η υλοποιημένη έκδοση αντιστοιχεί στην πιστοποιημένη αρχιτεκτονική, στα αξιολογημένα μέτρα και μηχανισμούς ασφάλειας και στις παραδοχές του Αντικειμένου Αξιολόγησης, καθώς και αν έχουν προκύψει αποκλίσεις, νέες εξαρτήσεις ή άλλες μεταβολές που επηρεάζουν την ασφάλεια. Η αξιολόγηση αυτή παραμένει τεκμηριωτική και δεν περιλαμβάνει τις δοκιμές ή επαληθεύσεις που αποκλείονται από το άρθρο 4 παρ. 4. Η συμπληρωματική τεκμηριωτική αξιολόγηση υπόκειται σε ανεξάρτητη επανεξέταση κατά το άρθρο 25 και ολοκληρώνεται με απόφαση του αρμόδιου οργάνου του άρθρου 26, χωρίς να απαιτείται νέα πλήρης αξιολόγηση εφόσον δεν διαπιστώνονται Ουσιώδεις Μεταβολές. Επαναβαθμολογούνται μόνο τα κριτήρια που επηρεάζονται από αποκλίσεις, νέες εξαρτήσεις ή άλλες μεταβολές. Οι βαθμολογίες των μη επηρεαζόμενων κριτηρίων διατηρούνται από την προηγούμενη αξιολόγηση, η συνολική Βαθμολογία Ασφάλειας επαναϋπολογίζεται και εφαρμόζονται εκ νέου οι προϋποθέσεις του άρθρου 26. Αν το αποτέλεσμα είναι θετικό, εκδίδεται επικαιροποιημένο πιστοποιητικό και η Κατάσταση Συστήματος μεταβάλλεται στο Μητρώο σε «Υλοποιημένο». Η αρχική ημερομηνία λήξης δεν μεταβάλλεται, εκτός αν διενεργηθεί πλήρης νέα αξιολόγηση. Αν διαπιστωθούν Ουσιώδεις Μεταβολές, εφαρμόζεται το άρθρο 29.

7. Για πιστοποιητικό με διάρκεια ισχύος μεγαλύτερη του ενός έτους διενεργείται ετήσια τεκμηριωτική επιτήρηση. Ο κάτοχος υποβάλλει, εντός δώδεκα μηνών από την έκδοση ή την τελευταία ετήσια επιτήρηση, ενημερωμένα στοιχεία τουλάχιστον για γνωστές ευπάθειες και την αντιμετώπισή τους, μεταβολές του Συστήματος, κατάσταση υποστήριξης ασφάλειας, κρίσιμες εξαρτήσεις και τυχόν ανοικτά ευρήματα ασφάλειας. Το ΚΕΜΕΑ αξιολογεί τεκμηριωτικά τα στοιχεία αυτά και μπορεί να ζητήσει συμπληρωματική αξιολόγηση ή να κινήσει τη διαδικασία του άρθρου 30. Η ετήσια επιτήρηση δεν περιλαμβάνει εργαστηριακές δοκιμές, δοκιμές διείσδυσης, έλεγχο πηγαίου κώδικα ή επιτόπια τεχνική επαλήθευση. Η ισχύς πιστοποιητικού που υπόκειται σε ετήσια τεκμηριωτική επιτήρηση τελεί υπό την προϋπόθεση εμπρόθεσμης υποβολής των απαιτούμενων στοιχείων. Η άπρακτη παρέλευση της προθεσμίας υποβολής επιφέρει αυτοδίκαιη αναστολή της ισχύος του πιστοποιητικού μέχρι την ολοκλήρωση της επιτήρησης, πάντως όχι πέραν του ανώτατου χρόνου αναστολής του άρθρου 30 παρ. 3. Η αναστολή καταχωρίζεται αμελλητί στο Μητρώο του άρθρου 33.

8. Η ανανέωση πιστοποιητικού γίνεται με νέα αίτηση. Το ΚΕΜΕΑ μπορεί να περιορίσει την αξιολόγηση στις μεταβολές που επήλθαν από την προηγούμενη αξιολόγηση και στα στοιχεία που επηρεάζονται από αυτές.

9. Το πιστοποιητικό δεν μεταβιβάζεται. Σε περίπτωση καθολικής διαδοχής του κατόχου ή μεταβίβασης της επιχειρηματικής δραστηριότητας στην οποία ανήκει το Αντικείμενο Αξιολόγησης, ο νέος φορέας μπορεί να ζητήσει, εντός τριάντα ημερών, την καταχώρισή του ως κατόχου στο Μητρώο του άρθρου 33, εφόσον αναλαμβάνει τις υποχρεώσεις της παρούσας και το Αντικείμενο Αξιολόγησης δεν μεταβάλλεται. Αν δεν υποβληθεί αίτημα εμπρόθεσμα, το πιστοποιητικό παύει να ισχύει.

Άρθρο 29

Ουσιώδεις Μεταβολές

1. Ο κάτοχος υποχρεούται να ενημερώνει το ΚΕΜΕΑ, πριν από την εφαρμογή τους, για κάθε μεταβολή που εμπίπτει στις κατηγορίες της παρ. 2. Οι διορθώσεις ευπαθειών γνωστοποιούνται κατά το άρθρο 28 παρ. 4.

2. Ουσιώδεις Μεταβολές μπορούν να αποτελούν ιδίως αλλαγές:

α) στην αρχιτεκτονική,
β) στους μηχανισμούς αυθεντικοποίησης,
γ) στους μηχανισμούς κρυπτογράφησης,
δ) στα χρησιμοποιούμενα πρωτόκολλα,
ε) σε κρίσιμες διεπαφές,
στ) σε κρίσιμα υποσυστήματα,
ζ) σε βασικές εξαρτήσεις, μέσω αντικατάστασης ή προσθήκης τους,
η) στον τρόπο αποθήκευσης ή επεξεργασίας δεδομένων,
θ) σε λογισμικό ή firmware που υλοποιεί λειτουργίες ασφάλειας, πέραν της διόρθωσης ευπαθειών.

3. Το ΚΕΜΕΑ κρίνει αν η μεταβολή είναι ουσιώδης και αν απαιτεί συμπληρωματική αξιολόγηση ή νέα πιστοποίηση.

4. Ο κάτοχος ενημερώνει το ΚΕΜΕΑ χωρίς αδικαιολόγητη καθυστέρηση για κάθε ευπάθεια που ενδέχεται να συνιστά Κρίσιμη Αδυναμία και για τα μέτρα αντιμετώπισής της.

5. Η συμπληρωματική αξιολόγηση διενεργείται κατά τα άρθρα 10 έως 26 και περιορίζεται στις μεταβολές και στα στοιχεία που επηρεάζονται από αυτές. Επαναβαθμολογούνται μόνο τα επηρεαζόμενα κριτήρια. Οι βαθμολογίες των μη επηρεαζόμενων κριτηρίων διατηρούνται από την προηγούμενη αξιολόγηση, η συνολική Βαθμολογία Ασφάλειας επαναϋπολογίζεται και εφαρμόζονται εκ νέου οι προϋποθέσεις του άρθρου 26. Η συμπληρωματική αξιολόγηση ολοκληρώνεται με απόφαση καταχώρισης της νέας έκδοσης, διαμόρφωσης ή αρχιτεκτονικής στο Μητρώο του άρθρου 33 ή με απόρριψη. Εφόσον η απόφαση είναι θετική, εκδίδεται επικαιροποιημένο πιστοποιητικό με την ίδια ημερομηνία λήξης. Κατά της απόφασης χωρεί ένσταση κατά το άρθρο 31.

6. Με την επιφύλαξη της ετήσιας τεκμηριωτικής επιτήρησης του άρθρου 28 παρ. 7, το ΚΕΜΕΑ δεν υποχρεούται σε διαρκή παρακολούθηση των πιστοποιημένων Συστημάτων. Η υποχρέωση ενημέρωσης για ευπάθειες βαρύνει τον κάτοχο κατά την παρ. 4.

Άρθρο 30

Αναστολή, ανάκληση, παραίτηση και αναφορές τρίτων

1. Το ΚΕΜΕΑ δύναται να αναστείλει ή να ανακαλέσει πιστοποιητικό όταν:

α) διαπιστωθεί ότι βασίστηκε σε ανακριβή ή παραπλανητικά στοιχεία,
β) πραγματοποιηθεί Ουσιώδης Μεταβολή που αναιρεί τις προϋποθέσεις της πιστοποίησης,
γ) γίνεται παραπλανητική χρήση του πιστοποιητικού,
δ) προκύψουν στοιχεία, ιδίως δημόσια γνωστή ευπάθεια, που καθιστούν πιθανή την ύπαρξη Κρίσιμης Αδυναμίας και ο κάτοχος δεν την αντιμετωπίσει ή δεν τεκμηριώσει ότι δεν επηρεάζεται εντός της προθεσμίας που τάσσει το ΚΕΜΕΑ,
ε) ο κάτοχος παραλείψει τη γνωστοποίηση κατά το άρθρο 28 παρ. 4 ή το άρθρο 29,
στ) μετά την αυτοδίκαιη αναστολή του άρθρου 28 παρ. 7, ο κάτοχος δεν συμμορφωθεί με την ετήσια τεκμηριωτική επιτήρηση εντός της προθεσμίας που τάσσει το ΚΕΜΕΑ,
ζ) λήξει η υποστήριξη ασφάλειας του Αντικειμένου Αξιολόγησης,
η) συντρέχει άλλος σοβαρός λόγος που συνδέεται άμεσα με την εγκυρότητα της πιστοποίησης.

2. Με την επιφύλαξη της αυτοδίκαιης αναστολής του άρθρου 28 παρ. 7, πριν από την αναστολή ή την ανάκληση ο κάτοχος καλείται να εκθέσει τις απόψεις του εντός δέκα ημερών. Εάν σοβαρός κίνδυνος επιβάλλει άμεση αναστολή, η ακρόαση ακολουθεί.

3. Η αναστολή δεν υπερβαίνει τους έξι μήνες. Αν οι λόγοι της αναστολής αρθούν, η ισχύς του πιστοποιητικού αποκαθίσταται, διαφορετικά το πιστοποιητικό ανακαλείται.

4. Η αναστολή, η αποκατάσταση και η ανάκληση καταχωρίζονται στο Μητρώο του άρθρου 33.

5. Κάθε ενδιαφερόμενος μπορεί να υποβάλει στο ΚΕΜΕΑ αναφορά για παραπλανητική χρήση πιστοποιητικού ή για στοιχεία που αφορούν την ασφάλεια πιστοποιημένου Συστήματος. Το ΚΕΜΕΑ εξετάζει την αναφορά και, εφόσον συντρέχει λόγος, κινεί τη διαδικασία του παρόντος άρθρου.

6. Σε περίπτωση παραίτησης του κατόχου, το πιστοποιητικό παύει να ισχύει από την υποβολή της παραίτησης και η παύση καταχωρίζεται στο Μητρώο του άρθρου 33.

Άρθρο 31

Ενστάσεις

1. Ο αιτών ή ο κάτοχος πιστοποιητικού μπορεί να ασκήσει αιτιολογημένη ένσταση κατά απόφασης που αφορά την πιστοποίηση. Η ένσταση ασκείται εντός δεκαπέντε ημερών από την κοινοποίηση της απόφασης.

2. Η ένσταση εξετάζεται από πρόσωπο ή όργανο, οριζόμενο κατά το άρθρο 5 παρ. 3, που δεν συμμετείχε στην αρχική αξιολόγηση, επανεξέταση ή απόφαση.

3. Η απόφαση επί της ένστασης είναι αιτιολογημένη και εκδίδεται εντός τριάντα ημερών από την άσκησή της.

4. Η άσκηση ένστασης δεν έχει ανασταλτικό αποτέλεσμα.

Άρθρο 32

Εμπιστευτικότητα

1. Ο Τεχνικός Φάκελος Ασφάλειας και τα συμπληρωματικά στοιχεία αντιμετωπίζονται ως εμπιστευτικά.

2. Ιδιαίτερη προστασία παρέχεται σε:

α) αρχιτεκτονικές συστημάτων,
β) τοπολογίες δικτύων,
γ) τεχνικές διαμορφώσεις,
δ) πληροφορίες για ευπάθειες,
ε) στοιχεία κρυπτογραφικών μηχανισμών και διαχείρισης κλειδιών,
στ) στοιχεία διεπαφών,
ζ) πληροφορίες των οποίων η αποκάλυψη μπορεί να αυξήσει τον κίνδυνο παραβίασης.

3. Δημοσιοποιούνται μόνο τα απολύτως αναγκαία στοιχεία για την επαλήθευση της ύπαρξης και ισχύος του πιστοποιητικού.

4. Το ΚΕΜΕΑ εφαρμόζει μέτρα ασφαλούς υποβολής, φύλαξης και πρόσβασης για τον Τεχνικό Φάκελο Ασφάλειας, με πρόσβαση μόνο των προσώπων που συμμετέχουν στη διαδικασία.

5. Η εμπιστευτικότητα ισχύει με την επιφύλαξη υποχρεώσεων κοινοποίησης που προβλέπονται από τον νόμο ή επιβάλλονται από δικαστική ή άλλη αρμόδια αρχή.

6. Το ΚΕΜΕΑ, ως Υπεύθυνος Επεξεργασίας, επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα που περιέχονται στην αίτηση, στον Τεχνικό Φάκελο Ασφάλειας και σε κάθε άλλο έγγραφο που υποβάλλεται σε αυτό ή συντάσσεται από αυτό στο πλαίσιο σύναψης και εκτέλεσης της σύμβασης πιστοποίησης, για σκοπούς διαχείρισης, παρακολούθησης και υλοποίησης της παρούσας και εκπλήρωσης των νόμιμων και κανονιστικών υποχρεώσεων του ΚΕΜΕΑ που συνδέονται με αυτήν. Η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 (ΓΚΠΔ), τον ν. 4624/2019 και την εκάστοτε ισχύουσα νομοθεσία. Τα στοιχεία του κατόχου καταχωρίζονται και τηρούνται στο δημόσια επαληθεύσιμο Μητρώο του άρθρου 33 για όσο χρονικό διάστημα απαιτείται για την εκπλήρωση των σκοπών της επεξεργασίας κατά το άρθρο 36 του παρόντος και των υποχρεώσεων τήρησης αρχείων που προβλέπονται από την κείμενη νομοθεσία. Για την άσκηση δικαιωμάτων πρόσβασης, διόρθωσης, διαγραφής, περιορισμού της επεξεργασίας και εναντίωσης, όπου αυτά εφαρμόζονται, είναι διαθέσιμη η ηλεκτρονική διεύθυνση *dpo@kemea-research.gr*. Παράλληλα, επισημαίνεται το δικαίωμα υποβολής καταγγελίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (www.dpa.gr).

7. Εάν από τα στοιχεία που τίθενται υπόψη του ΚΕΜΕΑ προκύπτει σοβαρή ευπάθεια που ενδέχεται να επηρεάζει και τρίτους, το ΚΕΜΕΑ ενημερώνει τον αιτούντα ή τον κάτοχο. Εφόσον η ευπάθεια δεν αντιμετωπίζεται σε εύλογο χρόνο και η γνωστοποίηση επιβάλλεται ή επιτρέπεται από την κείμενη νομοθεσία, το ΚΕΜΕΑ δύναται να ενημερώσει την κατά περίπτωση αρμόδια αρχή ή ομάδα απόκρισης σε περιστατικά ασφάλειας υπολογιστών (CSIRT), περιορίζοντας τη γνωστοποίηση στα απολύτως αναγκαία στοιχεία.

Άρθρο 33

Μητρώο πιστοποιημένων Συστημάτων

1. Το ΚΕΜΕΑ τηρεί Μητρώο των πιστοποιητικών που εκδίδει.

2. Για κάθε πιστοποιητικό καταχωρίζονται τουλάχιστον:

α) ο μοναδικός αριθμός,
β) ο κάτοχος (επωνυμία ή ονοματεπώνυμο),
γ) η ονομασία του Συστήματος,
δ) η έκδοση ή διαμόρφωση, καθώς και οι μεταγενέστερες εκδόσεις που καταχωρίζονται κατά το άρθρο 28 παρ. 4 και το άρθρο 29 παρ. 5,
ε) η Κατάσταση Συστήματος και οι μεταβολές της,
στ) η ημερομηνία έκδοσης,
ζ) η ημερομηνία λήξης,
η) η κατάσταση του πιστοποιητικού και οι μεταβολές της.

3. Το ΚΕΜΕΑ παρέχει δημόσια δυνατότητα επαλήθευσης της γνησιότητας, της ισχύος, της Κατάστασης Συστήματος και των καλυπτόμενων εκδόσεων κάθε πιστοποιητικού, κατόπιν αιτήματος και, από τη θέση της σε λειτουργία, μέσω ηλεκτρονικής εφαρμογής στον διαδικτυακό τόπο του ΚΕΜΕΑ. Η επαλήθευση διενεργείται με βάση τον μοναδικό αριθμό ή τον κωδικό ηλεκτρονικής επαλήθευσης του πιστοποιητικού και εμφανίζει μόνο τα στοιχεία των περ. α΄ έως η΄ της παρ. 2. Δεν δημοσιεύεται κατάλογος των πιστοποιητικών ούτε στοιχεία επικοινωνίας του κατόχου.

Άρθρο 34

Χρήση της πιστοποίησης

1. Ο κάτοχος μπορεί να αναφέρεται στην πιστοποίηση μόνο σε σχέση με το ακριβές Αντικείμενο Αξιολόγησης.

2. Απαγορεύεται η χρήση του πιστοποιητικού κατά τρόπο που δημιουργεί την εντύπωση ότι έχουν πιστοποιηθεί άλλες εκδόσεις, προϊόντα, υπηρεσίες ή ιδιότητες που δεν περιλαμβάνονται στο πεδίο του.

3. Μετά τη λήξη, αναστολή ή ανάκληση παύει κάθε δικαίωμα αναφοράς σε ενεργή πιστοποίηση.

4. Κάθε αναφορά στην πιστοποίηση συνοδεύεται από τον μοναδικό αριθμό του πιστοποιητικού. Το όνομα και το λογότυπο του ΚΕΜΕΑ χρησιμοποιούνται μόνο στη μορφή και υπό τους όρους που ορίζει το ΚΕΜΕΑ.

5. Απαγορεύεται η χρήση της Βαθμολογίας Ασφάλειας για συγκριτική προβολή έναντι άλλων συστημάτων. Απαγορεύεται επίσης κάθε σήμανση επί του προϊόντος που μπορεί να εκληφθεί ως σήμανση συμμόρφωσης κατά την ενωσιακή νομοθεσία.

6. Πιστοποιητικό που αφορά συγκεκριμένη τυποποιημένη έκδοση και διαμόρφωση Τεχνολογικού Συστήματος, κατόπιν αίτησης ή με συναίνεση του κατασκευαστή ή παρόχου, μπορεί να επικαλείται, εφόσον το επιτρέπει ο κάτοχος, και τρίτος που προσφέρει ή εγκαθιστά την ίδια έκδοση και διαμόρφωση του Τεχνολογικού Συστήματος, μόνο εφόσον δεν μεταβάλλονται η πιστοποιημένη διαμόρφωση, τα όρια του Αντικειμένου Αξιολόγησης και οι ουσιώδεις παραδοχές του περιβάλλοντος λειτουργίας. Ο τρίτος δεν αποκτά την ιδιότητα του κατόχου. Η επίκληση του πιστοποιητικού από τρίτο δεν συνιστά πιστοποίηση της συγκεκριμένης εγκατάστασης του τρίτου. Ο κάτοχος ευθύνεται για τη χρήση του πιστοποιητικού από τρίτους στους οποίους την επιτρέπει, και παραπλανητική χρήση από αυτούς λογίζεται ως παραπλανητική χρήση κατά το άρθρο 30 παρ. 1 περ. γ΄. Σε κάθε άλλη περίπτωση ο τρίτος μπορεί να υποβάλει δική του αίτηση κατά το άρθρο 6 παρ. 5.

Άρθρο 35

Οικονομικοί όροι

1. Η διαδικασία πιστοποίησης παρέχεται από το ΚΕΜΕΑ έναντι αμοιβής στο πλαίσιο συμβατικής σχέσης με τον αιτούντα. Το ύψος της αμοιβής καθορίζεται , με έγγραφη οικονομική προσφορά του ΚΕΜΕΑ βάσει κριτηρίων που εγκρίνονται από το Διοικητικό Συμβούλιο, σύμφωνα με τις διατάξεις του ν.3387/2005, όπως ισχύει και του Εσωτερικού Κανονισμού Λειτουργίας. Για τον υπολογισμό της αμοιβής λαμβάνονται ιδίως υπόψη η έκταση και η πολυπλοκότητα του Αντικειμένου Αξιολόγησης, ο όγκος και η πληρότητα του Τεχνικού Φακέλου Ασφάλειας και η τυχόν ανάγκη συνδρομής εξωτερικών εμπειρογνωμόνων.
2. Η οικονομική προσφορά αποστέλλεται στον αιτούντα μετά την υποβολή της αίτησης και του Τεχνικού Φακέλου Ασφάλειας, εφόσον έχουν υποβληθεί τα αναγκαία στοιχεία για την εκτίμηση του αντικειμένου και του κόστους της αξιολόγησης. Στην προσφορά προσδιορίζονται το ύψος της αμοιβής, ο τρόπος και ο χρόνος καταβολής της, οι τυχόν πρόσθετες χρεώσεις και οι προϋποθέσεις επιβολής τους, καθώς και ο ελάχιστος και ο μέγιστος εκτιμώμενος χρόνος έκδοσης της απόφασης, σύμφωνα με το άρθρο 26 παρ. 5. Η αποδοχή της προσφοράς από τον αιτούντα συνιστά αποδοχή των οικονομικών όρων της διαδικασίας πιστοποίησης.
3. Η αμοιβή καταβάλλεται σύμφωνα με τους όρους της αποδεκτής οικονομικής προσφοράς και δύναται να προβλέπεται η προκαταβολική καταβολή του συνόλου ή μέρους αυτής, πριν από την έναρξη της αξιολόγησης. Η είσπραξη, η καταχώριση και η διαχείριση των σχετικών ποσών πραγματοποιούνται σύμφωνα με τις εφαρμοστέες διατάξεις περί οικονομικής διαχείρισης και δημοσίου λογιστικού, τον Εσωτερικό Κανονισμό Λειτουργίας και τις εγκεκριμένες οικονομικές διαδικασίες του ΚΕ.ΜΕ.Α.
4. Η καταβολή της αμοιβής αφορά την παροχή υπηρεσιών αξιολόγησης και δεν εγγυάται τη χορήγηση πιστοποιητικού.

5. Σε περίπτωση ανάκλησης της αίτησης από τον αιτούντα ή αρχειοθέτησής της πριν την ολοκλήρωση της διαδικασίας, το ΚΕΜΕΑ δικαιούται την αμοιβή που αναλογεί στις υπηρεσίες που έχουν πράγματι παρασχεθεί έως τον χρόνο διακοπής, καθώς και την κάλυψη τυχόν αναγκαίων και τεκμηριωμένων δαπανών που έχουν πραγματοποιηθεί για την εκτέλεση της συγκεκριμένης αξιολόγησης, εφόσον αυτές προβλέπονται στην αποδεκτή οικονομική προσφορά. Τυχόν προκαταβληθέν ποσό που υπερβαίνει τις ανωτέρω οφειλές επιστρέφεται στον αιτούντα, σύμφωνα με τις εφαρμοστέες οικονομικές διαδικασίες του ΚΕ.ΜΕ.Α.
6. Κάθε ουσιώδης μεταβολή του αντικειμένου ή της έκτασης της αξιολόγησης, η οποία συνεπάγεται πρόσθετη αμοιβή, γνωστοποιείται προηγουμένως στον αιτούντα και προϋποθέτει την έγγραφη αποδοχή συμπληρωματικής οικονομικής προσφοράς. Χωρίς την αποδοχή αυτή δεν γεννάται υποχρέωση καταβολής πρόσθετης αμοιβής.
7. Οι διατάξεις του παρόντος άρθρου εφαρμόζονται αναλόγως στην καταχώριση εκδόσεων κατά το άρθρο 28 παρ. 4, στη συμπληρωματική τεκμηριωτική αξιολόγηση για μεταβολή της Κατάστασης Συστήματος κατά το άρθρο 28 παρ. 6, στην ετήσια τεκμηριωτική επιτήρηση κατά το άρθρο 28 παρ. 7, στη συμπληρωματική αξιολόγηση κατά το άρθρο 29 παρ. 5 και στην ανανέωση πιστοποιητικού.

Άρθρο 36

Τήρηση αρχείων

1. Το ΚΕΜΕΑ τηρεί αρχείο για κάθε διαδικασία πιστοποίησης.

2. Το αρχείο περιλαμβάνει την αίτηση, τον Τεχνικό Φάκελο Ασφάλειας, τα συμπληρωματικά στοιχεία, την Έκθεση Αξιολόγησης, την επανεξέταση, την απόφαση και το πιστοποιητικό, εφόσον εκδοθεί.

3. Ο Τεχνικός Φάκελος Ασφάλειας και τα συμπληρωματικά στοιχεία διατηρούνται όσο ισχύει το πιστοποιητικό και για πέντε έτη μετά τη λήξη, την ανάκληση ή την παύση του ή, αν δεν εκδοθεί πιστοποιητικό, για πέντε έτη από την απόφαση ή την αρχειοθέτηση της αίτησης. Στη συνέχεια καταστρέφονται με ασφαλή τρόπο, εκτός αν η διατήρησή τους επιβάλλεται από τον νόμο ή είναι αναγκαία σε εκκρεμή διαφορά. Τα λοιπά στοιχεία του αρχείου διατηρούνται σύμφωνα με τις ισχύουσες απαιτήσεις και τις εσωτερικές διαδικασίες του ΚΕΜΕΑ.

4. Οι εγγραφές του Μητρώου τηρούνται όσο ισχύει το πιστοποιητικό και για πέντε έτη μετά τη λήξη, την ανάκληση ή την παύση του.

Άρθρο 37

Ερμηνεία της Βαθμολογίας Ασφάλειας

1. Η Βαθμολογία Ασφάλειας αποτυπώνει το αποτέλεσμα της τεκμηριωτικής αξιολόγησης βάσει των στοιχείων που τέθηκαν υπόψη του ΚΕΜΕΑ κατά τον χρόνο της αξιολόγησης.

2. Βαθμολογία εκατό μονάδων δεν σημαίνει ότι το Σύστημα είναι απαλλαγμένο από ευπάθειες ή ότι δεν μπορεί να παραβιαστεί.

3. Η βαθμολογία δεν αποτελεί μέτρηση πιθανότητας παραβίασης ούτε ποσοτική εκτίμηση κινδύνου.

4. Η βαθμολογία χρησιμοποιείται αποκλειστικά για τους σκοπούς της παρούσας διαδικασίας πιστοποίησης. Το ΚΕΜΕΑ δεν ευθύνεται για τη χρήση της από τρίτους για άλλους σκοπούς.

Άρθρο 38

Έγκριση, έναρξη ισχύος και δημοσιοποίηση

1. Η παρούσα Διαδικασία Πιστοποίησης Τεχνολογικών Συστημάτων εγκρίνεται με απόφαση του Διοικητικού Συμβουλίου του ΚΕ.ΜΕ.Α., σύμφωνα με τις αρμοδιότητές του που απορρέουν από τον ν. 3387/2005, όπως ισχύει και τον Εσωτερικό Κανονισμό Λειτουργίας του.

2. Η παρούσα εφαρμόζεται στο πλαίσιο της συμβατικής παροχής υπηρεσιών πιστοποίησης από το ΚΕ.ΜΕ.Α., κατόπιν αίτησης του ενδιαφερομένου και ρητής αποδοχής των όρων της. Δεν θεσπίζει γενικώς υποχρεωτική διαδικασία πιστοποίησης ούτε επιβάλλει υποχρεώσεις σε τρίτους που δεν έχουν αποδεχθεί την εφαρμογή της.

3. Η παρούσα τίθεται σε ισχύ από την ημερομηνία που ορίζεται στην απόφαση έγκρισής της από το Διοικητικό Συμβούλιο και αναρτάται στην επίσημη ιστοσελίδα του ΚΕ.ΜΕ.Α., προκειμένου να διασφαλίζεται η διαφάνεια και η προηγούμενη ενημέρωση των ενδιαφερομένων. Οι όροι της καθίστανται δεσμευτικοί για τον εκάστοτε αιτούντα από την αποδοχή τους, σύμφωνα με τα προβλεπόμενα στην παρούσα.

4. Κάθε τροποποίηση της παρούσας εγκρίνεται από το Διοικητικό Συμβούλιο και δημοσιοποιείται κατά τον ίδιο τρόπο. Οι τροποποιήσεις εφαρμόζονται στις αιτήσεις που υποβάλλονται μετά την έναρξη ισχύος τους, εκτός εάν συμφωνηθεί ρητώς διαφορετικά με τον αιτούντα, με την επιφύλαξη της κείμενης νομοθεσίας.