26/02/2025
ESMA75-223375936-6132

Κατευθυντήριες γραμμές

Για τον καθορισμό ενωσιακών προτύπων σχετικά με τη διατήρηση συστημάτων και πρωτοκόλλων ασφαλούς πρόσβασης για τους προσφέροντες και τους επιδιώκοντες την εισαγωγή προς διαπραγμάτευση κρυπτοστοιχείων εκτός μαρκών με αναφορά σε περιουσιακά στοιχεία και μαρκών ηλεκτρονικού χρήματος

Πίνακας περιεχομένων

1 Πεδίο εφαρμογής 2

2 Νομοθετικές παραπομπές, συντομογραφίες και ορισμοί 3

2.1 Νομοθετικές παραπομπές 3

2.2 Συντομογραφίες 3

2.3 Ορισμοί 4

3 Σκοπός 4

4 Υποχρεώσεις συμμόρφωσης και υποβολής εκθέσεων 5

4.1 Καθεστώς των κατευθυντήριων γραμμών 5

4.2 Απαιτήσεις υποβολής εκθέσεων 5

5 Κατευθυντήριες γραμμές για τον καθορισμό ενωσιακών προτύπων σχετικά με τη διατήρηση συστημάτων και πρωτοκόλλων ασφαλούς πρόσβασης για τους προσφέροντες και τους επιδιώκοντες την εισαγωγή προς διαπραγμάτευση κρυπτοστοιχείων εκτός μαρκών με αναφορά σε περιουσιακά στοιχεία και μαρκών ηλεκτρονικού χρήματος 6

5.1 Κατευθυντήρια γραμμή 1: γενική αρχή της αναλογικότητας 6

5.2 Κατευθυντήρια γραμμή 2: διοικητικές ρυθμίσεις σχετικά με τα συστήματα και τα πρωτόκολλα ασφαλούς πρόσβασης 6

5.3 Κατευθυντήρια γραμμή 3: πρωτόκολλα ασφαλούς φυσικής πρόσβασης 8

5.4 Κατευθυντήρια γραμμή 4: πρωτόκολλα ασφαλούς πρόσβασης για συστήματα δικτύου και πληροφοριών 8

5.5 Κατευθυντήρια γραμμή 5: διαχείριση κρυπτογραφικών κλειδιών 9

1 Πεδίο εφαρμογής

Ποιος;

1. Οι παρούσες κατευθυντήριες γραμμές ισχύουν για τις αρμόδιες αρχές και τους «προσφέροντες», όπως ορίζονται στο άρθρο 3 παράγραφος 1 σημείο 13 του κανονισμού για τις αγορές κρυπτοστοιχείων (MiCA), καθώς και για τους επιδιώκοντες την εισαγωγή προς διαπραγμάτευση κρυπτοστοιχείων εκτός μαρκών με αναφορά σε περιουσιακά στοιχεία ή μαρκών ηλεκτρονικού χρήματος.

Τι;

2. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται σε σχέση με το άρθρο 14 παράγραφος 1 στοιχείο δ) του κανονισμού MiCA.

Πότε;

3. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται 60 ημερολογιακές ημέρες από την ημερομηνία δημοσίευσής τους στον δικτυακό τόπο της ESMA σε όλες τις επίσημες γλώσσες της ΕΕ.

2 Νομοθετικές παραπομπές, συντομογραφίες και ορισμοί

2.1 Νομοθετικές παραπομπές

DORA	Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011.[1]
MiCA	Κανονισμός (ΕΕ) 2023/1114 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 31ης Μαΐου 2023, για τις αγορές κρυπτοστοιχείων και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1093/2010 και (ΕΕ) αριθ. 1095/2010 και των οδηγιών 2013/36/ΕΕ και (ΕΕ) 2019/1937.[2]
Κανονισμός ESMA	Κανονισμός (ΕΕ) αριθ. 1095/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, σχετικά με τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/77/ΕΚ.[3]
Οδηγία NIS2	Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148.[4]

2.2 Συντομογραφίες

ART	Μάρκα(-ες) με αναφορά σε περιουσιακά στοιχεία
EMT	Μάρκα(-ες) ηλεκτρονικού χρήματος
ESMA	Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών
ΕΕ	Ευρωπαϊκή Ένωση
Επιτροπή	Ευρωπαϊκή Επιτροπή

[1] ΕΕ L 333 της 14.12.2022, σ. 1–79.
[2] ΕΕ L 150 της 9.6.2023, σ. 40.
[3] ΕΕ L 331 της 15.12.2010, σ. 84.
[4] ΕΕ L 333 της 12.12.2022, σ. 80-133.

2.3 Ορισμοί

έλεγχος πρόσβασης	έλεγχοι με τους οποίους διασφαλίζεται ότι η φυσική και λογική πρόσβαση σε πόρους ΤΠΕ επιτρέπεται και περιορίζεται με βάση τις απαιτήσεις επιχειρησιακής ασφάλειας και ασφάλειας των πληροφοριών.[5]
κίνδυνος ΤΠΕ	«κίνδυνος ΤΠΕ» όπως ορίζεται στο άρθρο 3 σημείο 5) του κανονισμού DORA.
πόρος ΤΠΕ	«πόρος ΤΠΕ» όπως ορίζεται στο άρθρο 3 σημείο 7 του κανονισμού DORA.
προσφέροντες και επιδιώκοντες την εισαγωγή προς διαπραγμάτευση	συντομευμένη μορφή του όρου «προσφέροντες και επιδιώκοντες την εισαγωγή προς διαπραγμάτευση κρυπτοστοιχείων εκτός μαρκών με αναφορά σε περιουσιακά στοιχεία και μαρκών ηλεκτρονικού χρήματος», για τους σκοπούς των παρουσών κατευθυντήριων γραμμών.
σύστημα δικτύου και πληροφοριών	«σύστημα δικτύου και πληροφοριών» όπως ορίζεται στο άρθρο 6 σημείο 1) της οδηγίας NIS2.

3 Σκοπός

4. Οι παρούσες κατευθυντήριες γραμμές, οι οποίες καταρτίστηκαν σε συνεργασία με την Ευρωπαϊκή Αρχή Τραπεζών, βασίζονται στο άρθρο 14 παράγραφος 1 στοιχείο δ) του κανονισμού MiCA. Σκοπός αυτών των κατευθυντήριων γραμμών είναι να καθορίσουν τα κατάλληλα ενωσιακά πρότυπα για τους προσφέροντες και τους επιδιώκοντες την εισαγωγή προς διαπραγμάτευση όσον αφορά τη διατήρηση των συστημάτων και των πρωτοκόλλων ασφαλούς πρόσβασης, συμπεριλαμβανομένων των πολιτικών και των διαδικασιών. Οι παρούσες κατευθυντήριες γραμμές αποσκοπούν επίσης στην προώθηση μεγαλύτερης σύγκλισης στην ερμηνεία και την εφαρμογή των διατάξεων του MiCA που ισχύουν για τους προσφέροντες και τους επιδιώκοντες την εισαγωγή προς διαπραγμάτευση.

[5] *ISO/IEC 29146:2016 Τεχνολογία πληροφοριών — Τεχνικές ασφάλειας — Πλαίσιο για τη διαχείριση της πρόσβασης*. Διεθνής Οργανισμός Τυποποίησης, 2016.

4 Υποχρεώσεις συμμόρφωσης και υποβολής εκθέσεων

4.1 Καθεστώς των κατευθυντήριων γραμμών

5. Σύμφωνα με το άρθρο 16 του κανονισμού ESMA, οι αρμόδιες αρχές πρέπει να καταβάλλουν κάθε δυνατή προσπάθεια για να εποπτεύουν την εφαρμογή των παρουσών κατευθυντήριων γραμμών και οι προσφέροντες ή οι επιδιώκοντες την εισαγωγή προς διαπραγμάτευση πρέπει να καταβάλλουν κάθε δυνατή προσπάθεια για να συμμορφωθούν με αυτές.

6. Οι αρμόδιες αρχές προς τις οποίες απευθύνονται οι παρούσες κατευθυντήριες γραμμές θα πρέπει να ενσωματώσουν αυτές τις κατευθυντήριες γραμμές, κατά περίπτωση, στα οικεία εθνικά νομικά και/ή εποπτικά πλαίσια, ακόμη και όταν συγκεκριμένες κατευθυντήριες γραμμές απευθύνονται πρωτίστως σε συμμετέχοντες στις αγορές κρυπτοστοιχείων στις δικαιοδοσίες τους. Σε αυτήν την περίπτωση, οι αρμόδιες αρχές πρέπει να διασφαλίζουν, μέσω της άσκησης της εποπτείας τους, ότι οι συμμετέχοντες στις χρηματοοικονομικές αγορές συμμορφώνονται προς τις κατευθυντήριες γραμμές.

4.2 Απαιτήσεις υποβολής εκθέσεων

7. Εντός δύο μηνών από την ημερομηνία δημοσίευσης των κατευθυντήριων γραμμών στον δικτυακό τόπο της ESMA σε όλες τις επίσημες γλώσσες της ΕΕ, οι αρμόδιες αρχές που καλούνται να εφαρμόσουν τις παρούσες κατευθυντήριες γραμμές πρέπει να ενημερώσουν την ESMA εάν i) συμμορφώνονται, ii) δεν συμμορφώνονται, αλλά προτίθενται να συμμορφωθούν, ή iii) δεν συμμορφώνονται και δεν προτίθενται να συμμορφωθούν με τις κατευθυντήριες γραμμές.

8. Σε περίπτωση μη συμμόρφωσης, οι αρμόδιες αρχές πρέπει επίσης να κοινοποιούν στην ESMA, εντός δύο μηνών από την ημερομηνία δημοσίευσης των κατευθυντήριων γραμμών στον δικτυακό τόπο της ESMA σε όλες τις επίσημες γλώσσες της ΕΕ, τους λόγους για τους οποίους δεν συμμορφώνονται με τις κατευθυντήριες γραμμές.

9. Υπόδειγμα για την κοινοποίηση διατίθεται στον δικτυακό τόπο της ESMA. Αφού συμπληρωθεί, το υπόδειγμα διαβιβάζεται στην ESMA.

10. Οι προσφέροντες και οι επιδιώκοντες την εισαγωγή προς διαπραγμάτευση δεν υποχρεούνται να αναφέρουν εάν συμμορφώνονται ή όχι με τις παρούσες κατευθυντήριες γραμμές.

5 Κατευθυντήριες γραμμές για τον καθορισμό ενωσιακών προτύπων σχετικά με τη διατήρηση συστημάτων και πρωτοκόλλων ασφαλούς πρόσβασης για τους προσφέροντες και τους επιδιώκοντες την εισαγωγή προς διαπραγμάτευση κρυπτοστοιχείων εκτός μαρκών με αναφορά σε περιουσιακά στοιχεία και μαρκών ηλεκτρονικού χρήματος

5.1 Κατευθυντήρια γραμμή 1: γενική αρχή της αναλογικότητας

11. Οι προσφέροντες και οι επιδιώκοντες την εισαγωγή προς διαπραγμάτευση πρέπει να καταβάλλουν κάθε δυνατή προσπάθεια για να συμμορφώνονται με τις παρούσες κατευθυντήριες γραμμές κατά τρόπο αναλογικό και λαμβάνοντας υπόψη το μέγεθος του οργανισμού, το συνολικό προφίλ κινδύνου του, καθώς και τη φύση, το πεδίο και την πολυπλοκότητα των δραστηριοτήτων ή των λειτουργιών του.

5.2 Κατευθυντήρια γραμμή 2: διοικητικές ρυθμίσεις σχετικά με τα συστήματα και τα πρωτόκολλα ασφαλούς πρόσβασης

Διοικητικές ρυθμίσεις

12. Ο προσφέρων ή ο επιδιώκων την εισαγωγή προς διαπραγμάτευση θα πρέπει να εξασφαλίζει την ύπαρξη κατάλληλου πλαισίου εσωτερικής διακυβέρνησης και εσωτερικού ελέγχου για τη διατήρηση των συστημάτων δικτύου και πληροφοριών του και τον μετριασμό των κινδύνων ΤΠΕ. Ο προσφέρων ή ο επιδιώκων την εισαγωγή προς διαπραγμάτευση θα πρέπει επίσης να ορίζει σαφείς ρόλους και αρμοδιότητες για τις θέσεις που είναι υπεύθυνες για τη διαχείριση του κινδύνου ΤΠΕ.

13. Ο προσφέρων ή ο επιδιώκων την εισαγωγή προς διαπραγμάτευση θα πρέπει να διασφαλίζει ότι οι δεξιότητες του προσωπικού του και οι οικονομικοί του πόροι είναι επαρκείς για να υποστηρίξουν τις ρυθμίσεις διαχείρισης κινδύνων ΤΠΕ, ιδίως όσον αφορά το προσωπικό που είναι υπεύθυνο για τη διατήρηση των συστημάτων δικτύου και πληροφοριών και τους ελέγχους πρόσβασης, σε συνεχή βάση. Επιπλέον, ο προσφέρων ή ο επιδιώκων την εισαγωγή προς διαπραγμάτευση θα πρέπει να διασφαλίζει ότι τα σχετικά μέλη του προσωπικού, συμπεριλαμβανομένων των προσώπων που κατέχουν καίριες θέσεις, λαμβάνουν περιοδικά κατάλληλη εκπαίδευση σχετικά με τους κινδύνους ΤΠΕ.

14. Το διοικητικό όργανο του προσφέροντος ή του επιδιώκοντος την εισαγωγή προς διαπραγμάτευση θα πρέπει να είναι υπεύθυνο για τον καθορισμό, την έγκριση και την εποπτεία της εφαρμογής των ρυθμίσεων διαχείρισης κινδύνου ΤΠΕ του οργανισμού,

μεταξύ άλλων όσον αφορά τα συστήματα δικτύου και πληροφοριών και τους ελέγχους πρόσβασης.

Ρόλοι και αρμοδιότητες

15. Ο προσφέρων ή ο επιδιώκων την εισαγωγή προς διαπραγμάτευση θα πρέπει να αναθέσει στο προσωπικό του οργανισμού την ευθύνη για τον κατάλληλο εντοπισμό, τη διαχείριση και την εποπτεία των κινδύνων ΤΠΕ. Θα πρέπει να εξασφαλίζει ότι το προσωπικό που είναι υπεύθυνο για τη διαχείριση των κινδύνων ΤΠΕ και των λειτουργιών ασφάλειας εφαρμόζει κατάλληλες ρυθμίσεις για τον εντοπισμό, την παρακολούθηση, την αξιολόγηση και την αναφορά των εν λόγω κινδύνων ΤΠΕ.

16. Ο προσφέρων ή ο επιδιώκων την εισαγωγή προς διαπραγμάτευση θα πρέπει να εξασφαλίζει ότι το προσωπικό που είναι υπεύθυνο για τη διαχείριση των κινδύνων ΤΠΕ που σχετίζονται με τα συστήματα δικτύου και πληροφοριών και τους ελέγχους πρόσβασης είναι σε θέση να διασφαλίσει ότι οι εντοπιζόμενοι κίνδυνοι ΤΠΕ παρακολουθούνται, αξιολογούνται και αναφέρονται στο διοικητικό όργανο.

17. Ο προσφέρων ή ο επιδιώκων την εισαγωγή προς διαπραγμάτευση θα πρέπει να ορίζει και να αναθέτει βασικούς ρόλους και αρμοδιότητες για τη θέσπιση ρυθμίσεων με σκοπό:

    i. τον εντοπισμό και την αξιολόγηση των κινδύνων ΤΠΕ, συμπεριλαμβανομένων εκείνων που σχετίζονται με τις υπηρεσίες ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών, στους οποίους εκτίθεται ο οργανισμός·

    ii. τον καθορισμό μέτρων για τον μετριασμό των κινδύνων, συμπεριλαμβανομένων ελέγχων για τον μετριασμό των κινδύνων τρίτων παρόχων ΤΠΕ·

    iii. την παρακολούθηση της αποτελεσματικότητας των μέτρων που αναφέρονται στο σημείο ii. και την ανάληψη δράσης για τη διόρθωση των μέτρων, εφόσον απαιτείται·

    iv. την υποβολή εκθέσεων στο διοικητικό όργανο σχετικά με τους κινδύνους ΤΠΕ και τα μέτρα μετριασμού·

    v. τον εντοπισμό και την αξιολόγηση τυχόν κίνδυνων ΤΠΕ που προκύπτουν από οποιαδήποτε μείζονα αλλαγή στα συστήματα δικτύου και πληροφοριών ή στις υπηρεσίες ΤΠΕ (και όταν παρέχονται από τρίτους), ή μετά από οποιοδήποτε σημαντικό συμβάν σχετικό με τη λειτουργία ή την ασφάλεια·

    vi. τη διαχείριση των κρυπτογραφικών κλειδιών καθ’ όλη τη διάρκεια του κύκλου ζωής τους.

5.3 Κατευθυντήρια γραμμή 3: πρωτόκολλα ασφαλούς φυσικής πρόσβασης

18. Οι προσφέροντες και οι επιδιώκοντες την εισαγωγή προς διαπραγμάτευση θα πρέπει να καθορίζουν, να τεκμηριώνουν και να εφαρμόζουν μέτρα φυσικής ασφάλειας για την προστασία των εγκαταστάσεων, των κέντρων δεδομένων και των ευαίσθητων περιοχών τους από μη εξουσιοδοτημένη πρόσβαση και από περιβαλλοντικούς κινδύνους. Ο προσφέρων ή ο επιδιώκων την εισαγωγή προς διαπραγμάτευση θα πρέπει να τηρεί αρχείο κάθε εισόδου στις εγκαταστάσεις εκείνες για τις οποίες απαιτείται άδεια πρόσβασης.

19. Η φυσική πρόσβαση σε συστήματα δικτύου και πληροφοριών θα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα σύμφωνα με τις αρχές της ανάγκης γνώσης και των ελάχιστων προνομίων, και σε ειδικές περιπτώσεις. Η άδεια θα πρέπει να χορηγείται σύμφωνα με τα καθήκοντα και τις αρμοδιότητες του εξουσιοδοτημένου ατόμου και να περιορίζεται σε άτομα που είναι κατάλληλα εκπαιδευμένα και παρακολουθούνται δεόντως. Η άδεια φυσικής πρόσβασης θα πρέπει να επανεξετάζεται περιοδικά και να ανακαλείται όταν δεν απαιτείται πλέον.

20. Τα κατάλληλα μέτρα για την προστασία από περιβαλλοντικούς κινδύνους θα πρέπει να είναι ανάλογα με τη σημασία των κτιρίων και την κρισιμότητα των λειτουργιών ή των συστημάτων δικτύου και πληροφοριών που βρίσκονται στα εν λόγω κτίρια.

5.4 Κατευθυντήρια γραμμή 4: πρωτόκολλα ασφαλούς πρόσβασης για συστήματα δικτύου και πληροφοριών

21. Η λογική πρόσβαση στα συστήματα δικτύου και πληροφοριών θα πρέπει να περιορίζεται σε εξουσιοδοτημένα άτομα που ορίζονται από τον προσφέροντα ή τον επιδιώκοντα την εισαγωγή προς διαπραγμάτευση. Η άδεια θα πρέπει να χορηγείται σύμφωνα με τα καθήκοντα και τις αρμοδιότητες του μέλους του προσωπικού και να περιορίζεται σε άτομα που είναι κατάλληλα εκπαιδευμένα και των οποίων η πρόσβαση στα συστήματα παρακολουθείται δεόντως. Οι προσφέροντες και οι επιδιώκοντες την εισαγωγή προς διαπραγμάτευση θα πρέπει να θέτουν σε εφαρμογή ελέγχους που περιορίζουν αξιόπιστα την πρόσβαση στα συστήματα δικτύου και πληροφοριών σε άτομα που υπόκεινται σε νόμιμες επιχειρησιακές απαιτήσεις. Η ηλεκτρονική πρόσβαση μέσω εφαρμογών σε δεδομένα και συστήματα θα πρέπει να περιορίζεται στο ελάχιστο που απαιτείται για την παροχή της σχετικής υπηρεσίας.

22. Οι προσφέροντες και οι επιδιώκοντες την εισαγωγή προς διαπραγμάτευση θα πρέπει να θέτουν σε εφαρμογή ισχυρούς ελέγχους για την προνομιακή πρόσβαση στα συστήματα, περιορίζοντας αυστηρά την πρόσβαση και εποπτεύοντας στενά το προσωπικό με αυξημένα δικαιώματα πρόσβασης στο σύστημα. Θα πρέπει να εφαρμόζονται έλεγχοι όπως η πρόσβαση βάσει ρόλου, η καταγραφή και η επανεξέταση των δραστηριοτήτων των προνομιούχων χρηστών συστημάτων δικτύου και

πληροφοριών, η ισχυρή επαλήθευση ταυτότητας και η παρακολούθηση των ανωμαλιών. Ο προσφέρων ή ο επιδιώκων την εισαγωγή προς διαπραγμάτευση θα πρέπει να διαχειρίζεται τα δικαιώματα πρόσβασης σε πληροφοριακούς πόρους και στα συστήματα υποστήριξής τους βάσει της αρχής της ανάγκης γνώσης και των ελάχιστων προνομίων. Τα δικαιώματα λογικής πρόσβασης θα πρέπει να επανεξετάζονται περιοδικά και να ανακαλούνται όταν δεν είναι πλέον απαραίτητα.

23. Τα αρχεία καταγραφής πρόσβασης θα πρέπει να διατηρούνται για χρονικό διάστημα ανάλογο με την κρισιμότητα των προσδιοριζόμενων επιχειρησιακών λειτουργιών, των υποστηρικτικών διαδικασιών και των πληροφοριακών πόρων, με την επιφύλαξη των απαιτήσεων διατήρησης που ορίζονται στην ενωσιακή και εθνική νομοθεσία. Οι προσφέροντες και οι επιδιώκοντες την εισαγωγή προς διαπραγμάτευση θα πρέπει να χρησιμοποιούν αυτές τις πληροφορίες για να διευκολύνουν τον εντοπισμό και τη διερεύνηση ανώμαλων δραστηριοτήτων που έχουν εντοπιστεί κατά την παροχή των υπηρεσιών τους.

24. Η απομακρυσμένη διοικητική πρόσβαση σε κρίσιμους πόρους ΤΠΕ θα πρέπει να επιτρέπεται μόνο με βάση την ανάγκη γνώσης και τα ελάχιστα προνόμια, και μόνο όταν υπάρχουν ισχυρές λύσεις επαλήθευσης ταυτότητας.

25. Η λειτουργία προϊόντων, εργαλείων και διαδικασιών που σχετίζονται με τις διαδικασίες ελέγχου της πρόσβασης θα πρέπει να προστατεύει τις εν λόγω διαδικασίες ελέγχου της πρόσβασης από την υπονόμευση ή την παράκαμψη. Αυτό περιλαμβάνει την εγγραφή, την παράδοση, την ανάκληση και την απόσυρση των αντίστοιχων προϊόντων, εργαλείων και διαδικασιών.

5.5 Κατευθυντήρια γραμμή 5: διαχείριση κρυπτογραφικών κλειδιών

26. Ο προσφέρων ή ο επιδιώκων την εισαγωγή προς διαπραγμάτευση θα πρέπει να είναι υπεύθυνος για τη διαχείριση των κρυπτογραφικών κλειδιών στο πλαίσιο των ρόλων και των αρμοδιοτήτων που ανατίθενται στο βασικό προσωπικό για κινδύνους ΤΠΕ. Το εν λόγω προσωπικό του προσφέροντος ή των επιδιωκόντων την εισαγωγή προς διαπραγμάτευση θα πρέπει να είναι υπεύθυνο για τη διαχείριση των κρυπτογραφικών κλειδιών καθ' όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένης της δημιουργίας, ανανέωσης, αποθήκευσης, δημιουργίας αντιγράφων ασφαλείας, αρχειοθέτησης, ανάκτησης, διαβίβασης, απόσυρσης, ανάκλησης και καταστροφής των κλειδιών.

27. Οι προσφέροντες και οι επιδιώκοντες την εισαγωγή προς διαπραγμάτευση θα πρέπει να προσδιορίζουν και να εφαρμόζουν ελέγχους για την προστασία των κρυπτογραφικών κλειδιών καθ’ όλη τη διάρκεια του κύκλου ζωής τους από απώλεια, μη εξουσιοδοτημένη πρόσβαση, γνωστοποίηση και τροποποίηση.

28. Οι προσφέροντες και οι επιδιώκοντες την εισαγωγή προς διαπραγμάτευση θα πρέπει να αναπτύσσουν και να εφαρμόζουν μεθόδους για την αντικατάσταση των κρυπτογραφικών κλειδιών σε περίπτωση απώλειας, έκθεσης σε κίνδυνο ή ζημίας.

29. Οι προσφέροντες και οι επιδιώκοντες την εισαγωγή προς διαπραγμάτευση θα πρέπει να δημιουργούν και να τηρούν μητρώο για όλα τα πιστοποιητικά και τις συσκευές αποθήκευσης πιστοποιητικών τουλάχιστον για τους κρίσιμους πόρους ΤΠΕ. Το μητρώο θα πρέπει να επικαιροποιείται.

30. Οι προσφέροντες και οι επιδιώκοντες την εισαγωγή προς διαπραγμάτευση θα πρέπει να μεριμνούν για την άμεση ανανέωση των πιστοποιητικών πριν από τη λήξη τους.