					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P18					Τίτλος εγγράφου: **Πολιτική Κρυπτογραφικών Ελέγχων**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 01.01.2025			Ιδιοκτήτης εγγράφου:							
X	Πολιτική		Πρότυπο		Διαδικασία		Έντυπο		Μητρώο		Άλλο	

Ιστορικό αναθεωρήσεων				
Αριθμός αναθεώρησης	**Ημερομηνία αναθεώρησης**	**Αλλαγές**	**Ελέγχθηκε από**	**Ιδιοκτήτης διεργασίας**

Εγκρίσεις			
Όνομα	**Θέση**	**Ημερομηνία**	**Υπογραφή**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Clause 8	-
ISO/IEC 27002:2022	Controls 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12 έως SC-17, SC-28, SC-28(1), SC-12(3)	-
ΓΚΠΔ της ΕΕ	Άρθρο 32, Άρθρα 33–34, Αιτιολογική σκέψη 83	-
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(d)	-
Κανονισμός DORA της ΕΕ	Άρθρα 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει υποχρεωτικές απαιτήσεις για την ασφαλή και σύμφωνη με τις υποχρεώσεις συμμόρφωσης χρήση κρυπτογραφικών ελέγχων σε ολόκληρο τον οργανισμό, ώστε να διασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα ευαίσθητων και ρυθμιζόμενων πληροφοριών.

1.2 Η χρήση κρυπτογραφίας αποτελεί θεμέλιο της εμπιστοσύνης στις λειτουργίες ασφάλειας δεδομένων, υποστηρίζει τις ασφαλείς επικοινωνίες, επιβάλλει τον έλεγχο πρόσβασης και επιτρέπει τη συμμόρφωση με κανονιστικές απαιτήσεις μέσω αποτελεσματικών πρακτικών κρυπτογράφησης και διαχείρισης κλειδιών.

1.3 Η παρούσα πολιτική ευθυγραμμίζεται με το ISO/IEC 27001:2022 Clause 8.1 και το Annex A Control 8.24 και υποστηρίζει νομικές και επιχειρησιακές υποχρεώσεις βάσει του Άρθρου 32 του ΓΚΠΔ της ΕΕ, του Άρθρου 6(2)(d) του Κανονισμού DORA της ΕΕ και του Άρθρου 21 της Οδηγίας NIS2 της ΕΕ. Υποστηρίζει επίσης τους στόχους του COBIT 2019 για υπηρεσίες ασφάλειας και προστασία πληροφοριακών περιουσιακών στοιχείων.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλες τις οργανωτικές μονάδες, επιχειρησιακές λειτουργίες, μέλη του προσωπικού και τρίτους παρόχους υπηρεσιών που εμπλέκονται στη χρήση, διαχείριση ή υλοποίηση κρυπτογραφικών εργαλείων και μεθόδων.

2.2 Τα περιβάλλοντα που καλύπτονται περιλαμβάνουν περιβάλλοντα παραγωγής, ανάπτυξης, σταδιοποίησης, αντιγράφων ασφαλείας και αποκατάστασης καταστροφών, στα οποία ευαίσθητα δεδομένα μεταδίδονται, υποβάλλονται σε επεξεργασία ή αποθηκεύονται.

2.3 Το πεδίο εφαρμογής περιλαμβάνει όλα τα κρυπτογραφικά συστατικά και τις περιπτώσεις χρήσης, συμπεριλαμβανομένων ενδεικτικά των εξής:

2.3.1 Συμμετρική και ασύμμετρη κρυπτογράφηση

2.3.2 Ψηφιακές υπογραφές και πιστοποιητικά

2.3.3 Αλγόριθμοι κατακερματισμού

2.3.4 Ασφαλής δημιουργία, διανομή και καταστροφή κλειδιών

2.3.5 Transport Layer Security (TLS), πλήρης κρυπτογράφηση δίσκου (FDE) και κρυπτογράφηση σε επίπεδο API

2.3.6 Ασφαλή στοιχεία, όπως Hardware Security Modules (HSMs), Trusted Platform Modules (TPMs) και συστήματα διαχείρισης κλειδιών (KMS)

2.4 Η παρούσα πολιτική διέπει τη χρήση κρυπτογραφίας σε σχέση με:

2.4.1 Δεδομένα που έχουν ταξινομηθεί ως Εμπιστευτικά, Άκρως Εμπιστευτικά ή Ρυθμιζόμενα

2.4.2 Αυθεντικοποίηση και επαλήθευση ψηφιακής ταυτότητας

2.4.3 Ασφαλείς επικοινωνίες με εξωτερικά μέρη

2.4.4 Θεματοφυλακή κλειδιών και μηχανισμούς διπλού ελέγχου

3. Στόχοι

3.1 Να διασφαλίζεται ότι οι κρυπτογραφικές τεχνολογίες επιλέγονται, εγκρίνονται, υλοποιούνται και συντηρούνται σύμφωνα με τον επιχειρησιακό κίνδυνο, τα διεθνή πρότυπα και τις κανονιστικές απαιτήσεις.

3.2 Να θεσπίζεται τυποποιημένη δομή διακυβέρνησης για τη διαχείριση κρυπτογραφικών υπηρεσιών, με σαφή λογοδοσία για την υλοποίηση, την επικύρωση και τη διαχείριση εξαιρέσεων.

3.3 Να αποτρέπεται η μη εξουσιοδοτημένη χρήση, η εσφαλμένη παραμετροποίηση ή η απαξίωση κρυπτογραφικών αλγορίθμων και ελέγχων μέσω επίσημης διαδικασίας έγκρισης και ανασκόπησης.

3.4 Να διασφαλίζεται ότι οι κρυπτογραφικοί έλεγχοι ενσωματώνονται στη φάση σχεδιασμού συστημάτων και επικυρώνονται τακτικά, ώστε να αποτρέπεται η έκθεση δεδομένων, ο συμβιβασμός κλειδιών ή η υποβάθμιση πρωτοκόλλων.

3.5 Να εφαρμόζεται διαχείριση κύκλου ζωής για όλα τα κρυπτογραφικά κλειδιά, συμπεριλαμβανομένων της δημιουργίας, αποθήκευσης, χρήσης, περιοδικής αλλαγής, ανάκλησης και ασφαλούς καταστροφής.

3.6 Να επιτυγχάνεται συμμόρφωση με διεθνείς και περιφερειακές κανονιστικές απαιτήσεις που επιβάλλουν κρυπτογράφηση και ασφαλή χειρισμό δεδομένων, συμπεριλαμβανομένων του ΓΚΠΔ της ΕΕ, του Κανονισμού DORA της ΕΕ, της Οδηγίας NIS2 της ΕΕ και του COBIT 2019.

4. Ρόλοι και αρμοδιότητες

4.1 Υπεύθυνος Ασφάλειας Πληροφοριών / Επικεφαλής Ασφάλειας Πληροφοριών

4.1.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και διασφαλίζει την ευθυγράμμισή της με το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) και το ISO/IEC 27001 Annex A Control 8.24.

4.1.2 Εγκρίνει τη χρήση κρυπτογραφικών αλγορίθμων και ελέγχων και διασφαλίζει τη συμμόρφωση σε ολόκληρο τον οργανισμό.

4.2 Επικεφαλής Κρυπτογραφικών Λειτουργιών / Αρχιτέκτονας Ασφάλειας

4.2.1 Διαχειρίζεται τις καθημερινές λειτουργίες και τη διοίκηση των κρυπτογραφικών συστημάτων.

4.2.2 Τηρεί τον Κατάλογο Εγκεκριμένων Κρυπτογραφικών Μεθόδων (ACML) και το Μητρώο Διαχείρισης Κλειδιών.

4.2.3 Διενεργεί Ανασκοπήσεις Κρυπτογραφικού Σχεδιασμού (CDR) και αξιολογεί νέες κρυπτογραφικές τεχνολογίες.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Απαιτήσεις ανασκόπησης και επικαιροποίησης

9.1 Η παρούσα πολιτική πρέπει να ανασκοπείται ετησίως από τον Υπεύθυνο Ασφάλειας Πληροφοριών και τον Επικεφαλής Κρυπτογραφικών Λειτουργιών.

9.2 Τα εναύσματα ανασκόπησης περιλαμβάνουν:

9.2.1 Εντοπισμό κρυπτογραφικών ευπαθειών (π.χ. υποβάθμιση αλγορίθμου, κβαντικές επιθέσεις)

9.2.2 Κανονιστικές αλλαγές που απαιτούν επικαιροποιημένα πρότυπα κρυπτογράφησης

9.2.3 Επιχειρησιακά ή ελεγκτικά ευρήματα που αποκαλύπτουν κενά πολιτικής

9.2.4 Αναβαθμίσεις κρυπτογραφικών εργαλείων ή αρχιτεκτονικές αλλαγές

9.3 Οι επικαιροποιήσεις πρέπει να ελέγχονται ως προς την έκδοση στο Μητρώο Ελέγχου Εγγράφων ISMS και να κοινοποιούνται στους εξής:

9.3.1 Όλους τους διαχειριστές με ρόλους πρόσβασης σε κρυπτογραφικούς μηχανισμούς

9.3.2 Ομάδες ανάπτυξης και επικεφαλής DevSecOps

9.3.3 Τρίτους παρόχους που υπέχουν συμβατικές υποχρεώσεις κρυπτογράφησης

9.4 Η ομάδα ISMS πρέπει να διασφαλίζει ότι οι καταργημένες εκδόσεις αρχειοθετούνται και δεν αναφέρονται πλέον στις λειτουργικές διαδικασίες.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P1 - Πολιτική Ασφάλειας Πληροφοριών. Παρέχει το θεμελιώδες πλαίσιο διακυβέρνησης για όλα τα μέτρα ασφάλειας, συμπεριλαμβανομένης της εφαρμογής κρυπτογραφικών ελέγχων, της προστασίας περιουσιακών στοιχείων και των ασφαλών επικοινωνιών.

10.2 P4 - Πολιτική Ελέγχου Πρόσβασης. Διασφαλίζει ότι η λογική πρόσβαση σε κρυπτογραφικό υλικό και σε συστήματα διαχείρισης κρυπτογράφησης περιορίζεται αυστηρά βάσει της αρχής των ελάχιστων προνομίων και του Διαχωρισμού Καθηκόντων (SoD).

10.3 P6 - Πολιτική Διαχείρισης Κινδύνων. Υποστηρίζει την αξιολόγηση των κινδύνων που σχετίζονται με τους κρυπτογραφικούς ελέγχους και τεκμηριώνει τη στρατηγική αντιμετώπισης κινδύνων για εξαιρέσεις, απαξίωση αλγορίθμων ή σενάρια συμβιβασμού κλειδιών.

10.4 P12 - Πολιτική Διαχείρισης Περιουσιακών Στοιχείων. Επιβάλλει την ταξινόμηση ευαίσθητων δεδομένων και περιουσιακών στοιχείων υλικού, η οποία καθορίζει άμεσα τις κρυπτογραφικές απαιτήσεις και τις υποχρεώσεις θεματοφυλακής κλειδιών.

10.5 P13 - Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων. Ορίζει τα επίπεδα ταξινόμησης (π.χ. Εμπιστευτικό, Ρυθμιζόμενο) που ενεργοποιούν συγκεκριμένες απαιτήσεις κρυπτογράφησης σε μεταφορά και σε αποθήκευση.

10.6 P14 - Πολιτική Διατήρησης και Διάθεσης Δεδομένων. Καθορίζει διαδικασίες για την ασφαλή διάθεση κρυπτογραφημένων μέσων αποθήκευσης και κρυπτογραφικού υλικού κλειδιών στο τέλος του κύκλου ζωής.

10.7 P30 - Πολιτική Αντιμετώπισης Περιστατικών (P30). Περιγράφει τη στρατηγική απόκρισης του οργανισμού για συμβιβασμό κλειδιών, κακή χρήση πιστοποιητικών ή πιθανολογούμενες ευπάθειες αλγορίθμων, συμπεριλαμβανομένης της ταχείας ανάκλησης και της γνωστοποίησης παραβίασης.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 - Operational Planning and Control: Επιβάλλει τεχνικούς ελέγχους ασφάλειας, συμπεριλαμβανομένων κρυπτογραφικών μέτρων, ως μέρος των επιχειρησιακών δικλίδων ασφαλείας.

11.2 ISO/IEC 27002:2022

11.2.1 Controls 8.24, 8.25, 8: Παρέχει οδηγίες υλοποίησης για τους στόχους κρυπτογραφικών ελέγχων, την επιλογή αλγορίθμων, την εφαρμογή πρωτοκόλλων και τη διαχείριση του κύκλου ζωής πιστοποιητικών.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-12 - Cryptographic Key Establishment: Διασφαλίζει την ασφαλή δημιουργία και ανταλλαγή κλειδιών κρυπτογράφησης. Η P18 καθορίζει πώς πρέπει να δημιουργούνται και να ανταλλάσσονται συμμετρικά/ασύμμετρα κλειδιά με χρήση εγκεκριμένων αλγορίθμων και πρωτοκόλλων.

11.3.2 SC-13 - Cryptographic Protection: Επιβάλλει τη χρήση κρυπτογραφίας για την προστασία της εμπιστευτικότητας και της ακεραιότητας των πληροφοριών. Η P18 εφαρμόζει κρυπτογράφηση

σε αποθήκευση και σε μεταφορά βάσει της ταξινόμησης δεδομένων, με πρότυπα αλγορίθμων ευθυγραμμισμένα με το NIST FIPS 140-3.

11.3.3 SC-17 - Public Key Infrastructure (PKI) Certificates: Απαιτεί την υλοποίηση PKI για την υποστήριξη αυθεντικοποίησης και ψηφιακών υπογραφών. Η P18 περιγράφει τη χρήση PKI για την ασφάλεια επικοινωνιών, ταυτοτήτων συστημάτων και διαχειριστικής πρόσβασης.

11.3.4 SC-28, SC-28(1) - Protection of Information at Rest and in Transit: Απαιτεί κρυπτογράφηση δεδομένων όταν αυτά αποθηκεύονται ή μεταδίδονται μέσω μη έμπιστων δικτύων. Η P18 καθορίζει την εφαρμογή TLS, σηράγγων VPN, πλήρους κρυπτογράφησης δίσκου και ασφαλών μεθόδων αποθήκευσης για ευαίσθητα δεδομένα.

11.3.5 SC-12(3) - Symmetric Key Generation for Secure Storage and Distribution: Εστιάζει στην ασφαλή δημιουργία και διαχείριση συμμετρικών κλειδιών. Η P18 επιβάλλει τη χρήση ισχυρών γεννητριών τυχαίων αριθμών, πολιτικών περιοδικής αλλαγής κλειδιών και ασφαλών θησαυροφυλακίων κλειδιών για κρυπτογραφικές λειτουργίες.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 32 - Ασφάλεια της επεξεργασίας: Συνιστά ρητά την κρυπτογράφηση ως μέτρο μείωσης κινδύνου για δεδομένα προσωπικού χαρακτήρα.

11.4.2 Αιτιολογική σκέψη 83: Τονίζει την κρυπτογράφηση ως έλεγχο για την πρόληψη μη εξουσιοδοτημένης πρόσβασης σε δεδομένα.

11.4.3 Άρθρα 33 και 34: Η κρυπτογράφηση μπορεί να απαλλάσσει οργανισμούς από υποχρεωτικές γνωστοποιήσεις παραβίασης, εφόσον είναι αποτελεσματική.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(d): Απαιτεί τεχνικά και οργανωτικά μέτρα, συμπεριλαμβανομένων κρυπτογραφικών μέτρων προστασίας, για τη διατήρηση της διαθεσιμότητας και της ακεραιότητας των υπηρεσιών.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 6(2)(d): Τα χρηματοπιστωτικά ιδρύματα πρέπει να διασφαλίζουν τα δεδομένα, μεταξύ άλλων μέσω ισχυρής κρυπτογράφησης κρίσιμων πληροφοριών.

11.6.2 Άρθρο 11(1)(c): Επιβάλλει ασφαλείς ελέγχους επεξεργασίας δεδομένων για τρίτους παρόχους υπηρεσιών ΤΠΕ.

11.7 COBIT 2019

11.7.1 DSS05.01 - Protect Information Assets: Απαιτεί τη χρήση κρυπτογράφησης και διαχείρισης κλειδιών για την προστασία πληροφοριακών περιουσιακών στοιχείων από μη εξουσιοδοτημένη πρόσβαση.

11.7.2 DSS06.06 - Managed Security Testing: Συνιστά την επικύρωση συμμόρφωσης κρυπτογραφικών μηχανισμών ως μέρος αξιολογήσεων ευπαθειών.

11.7.3 MEA03 - Monitor, Evaluate and Assess Compliance: Επιβάλλει συνεχή διασφάλιση της αποτελεσματικότητας των κρυπτογραφικών ελέγχων.