					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P18S					Τίτλος εγγράφου: **Πολιτική Κρυπτογραφικών Ελέγχων P18S**							
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	Ρήτρα 8	
ISO/IEC 27002:2022	Έλεγχοι 8.24, 8.25	
NIST SP 800-53 Rev.5	SC-12 έως SC-17	
Οδηγία NIS2 της ΕΕ	Άρθρα 21(2)(d), 21(2)(e)	
Κανονισμός DORA της ΕΕ	Άρθρα 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
ΓΚΠΔ της ΕΕ	Άρθρα 32(1)(a), 34	

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει υποχρεωτικές απαιτήσεις για τη χρήση κρυπτογράφησης και κρυπτογραφικών ελέγχων με σκοπό την προστασία της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας επιχειρησιακών δεδομένων και δεδομένων προσωπικού χαρακτήρα.

1.2 Διασφαλίζει ότι τα κρυπτογραφικά εργαλεία χρησιμοποιούνται κατάλληλα σε συστήματα, συσκευές και υπηρεσίες υπολογιστικού νέφους σε περιβάλλον μικρής επιχείρησης.

1.3 Η παρούσα πολιτική υποστηρίζει άμεσα την πιστοποίηση ISO/IEC 27001:2022 και συμβάλλει στη συμμόρφωση του οργανισμού με τις νομικές υποχρεώσεις του βάσει του ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ και του Κανονισμού DORA της ΕΕ.

1.4 Οι κρυπτογραφικοί έλεγχοι που καλύπτονται περιλαμβάνουν την κρυπτογράφηση δεδομένων, τη διαχείριση πιστοποιητικών, τον ασφαλή χειρισμό κλειδιών και τα κρυπτογραφημένα αντίγραφα ασφαλείας.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται στα εξής:

2.1.1 Σε όλους τους εργαζομένους, αναδόχους και τρίτα μέρη που χειρίζονται δεδομένα της εταιρείας

2.1.2 Σε όλα τα επιχειρησιακά συστήματα, τις συσκευές τερματικού και τις πλατφόρμες υπολογιστικού νέφους που χρησιμοποιούνται για αποθήκευση, μετάδοση ή πρόσβαση σε εμπιστευτικές πληροφορίες

2.1.3 Σε όλα τα προσωπικά, οικονομικά, νομικά ή ευαίσθητα αρχεία που ταξινομούνται βάσει της πολιτικής ταξινόμησης δεδομένων του οργανισμού

2.1.4 Σε κάθε κρυπτογραφικό έλεγχο, συμπεριλαμβανομένων των μεθόδων κρυπτογράφησης, των κλειδιών, των διαπιστευτηρίων, των πιστοποιητικών και των μονάδων ασφάλειας

2.2 Η πολιτική καλύπτει δεδομένα σε αποθήκευση, δεδομένα κατά τη μεταφορά και δεδομένα σε χρήση. Ρυθμίζει επίσης την κρυπτογράφηση που χρησιμοποιείται για αντίγραφα ασφαλείας, το ηλεκτρονικό ταχυδρομείο, τις εξωτερικές μεταφορές δεδομένων και τους δημόσια προσβάσιμους ιστοτόπους.

3. Στόχοι

3.1 Να διασφαλίζεται ότι τα ευαίσθητα και ρυθμιζόμενα δεδομένα προστατεύονται ανά πάσα στιγμή με κατάλληλα κρυπτογραφικά μέτρα

3.2 Να καθορίζονται οι αρμοδιότητες για την επιλογή εργαλείων κρυπτογράφησης, τη ρύθμιση παραμέτρων και τη διαχείριση κλειδιών

3.3 Να προλαμβάνεται η μη εξουσιοδοτημένη πρόσβαση, η παραποίηση ή η διαρροή δεδομένων μέσω της εφαρμογής ασφαλών ελέγχων μετάδοσης και αποθήκευσης

3.4 Να διασφαλίζεται η συμμόρφωση με νομικές και κανονιστικές απαιτήσεις που επιβάλλουν την κρυπτογράφηση προσωπικών και επιχειρησιακών δεδομένων

3.5 Να διατηρούνται η ασφάλεια των λειτουργιών και η διαθεσιμότητα μέσω αποτελεσματικής διαχείρισης πιστοποιητικών και κρυπτογραφικών κλειδιών

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής

4.1.1 Εγκρίνει την παρούσα πολιτική και διασφαλίζει την εφαρμογή των κρυπτογραφικών απαιτήσεων

4.1.2 Ανασκοπεί εξαιρέσεις, γνωστοποιήσεις παραβιάσεων και τη συμμόρφωση των προμηθευτών με τις ρήτρες κρυπτογράφησης

4.1.3 Επαληθεύει ότι οι υπηρεσίες εξωτερικής ανάθεσης ή υπολογιστικού νέφους πληρούν τα πρότυπα κρυπτογράφησης

4.2 Εξωτερικός Πάροχος Υπηρεσιών Πληροφορικής / Διαχειριστής Πληροφορικής

4.2.1 Υλοποιεί και διατηρεί λύσεις κρυπτογράφησης (π.χ. πλήρη κρυπτογράφηση δίσκου, πιστοποιητικά SSL, VPN)

4.2.2 Διαχειρίζεται τον κύκλο ζωής των κρυπτογραφικών κλειδιών και τα εργαλεία ασφαλούς αποθήκευσης

4.2.3 Ρυθμίζει και παρακολουθεί την κρυπτογράφηση για την προστασία αντιγράφων ασφαλείας, ιστοτόπων και συσκευών

[... 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 Ετήσια ανασκόπηση

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά ετησίως από τον Γενικό Διευθυντή σε συντονισμό με τον Εξωτερικό Πάροχο Υπηρεσιών Πληροφορικής και τον Συντονιστή Ιδιωτικότητας.

9.2 Εναύσματα ενδιάμεσης ανασκόπησης

9.2.1 Ανασκοπήσεις πρέπει επίσης να διενεργούνται εάν:

9.2.1.1 Αλλάξουν τα κρυπτογραφικά πρότυπα ή πρωτόκολλα (π.χ. κατάργηση αλγορίθμου)

9.2.1.2 Εισαχθούν νέα συστήματα ή υπηρεσίες υπολογιστικού νέφους

9.2.1.3 Μια παραβίαση ή ένα περιστατικό αφορά παραβιασμένο κλειδί ή πιστοποιητικό

9.2.1.4 Νομικές ή κανονιστικές επικαιροποιήσεις επηρεάζουν τις απαιτήσεις κρυπτογράφησης

9.3 Έλεγχος εκδόσεων και επικοινωνία

9.3.1 Όλες οι αλλαγές πολιτικής πρέπει να τεκμηριώνονται σε αρχείο ελέγχου εκδόσεων

9.3.2 Το προσωπικό πρέπει να ενημερώνεται για τις επικαιροποιήσεις και οι προηγούμενες εκδόσεις πρέπει να αρχειοθετούνται

9.3.3 Η τελευταία εγκεκριμένη έκδοση πρέπει να αποθηκεύεται στο κεντρικό αποθετήριο πολιτικών

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική πρέπει να εφαρμόζεται σε συνδυασμό με τις ακόλουθες πολιτικές SME:

10.1.1 P12S – Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Διασφαλίζει ότι εφαρμόζεται κρυπτογράφηση σε ταξινομημένα περιουσιακά στοιχεία κατά την αποθήκευση, τη μεταφορά και τη διάθεσή τους.

10.1.2 P14S – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Καθορίζει περιόδους διατήρησης και απαιτεί κρυπτογραφημένη αποθήκευση δεδομένων έως την ασφαλή διαγραφή τους.

10.1.3 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Ευθυγραμμίζει την κρυπτογράφηση με τις αρχές προστασίας δεδομένων και τις κανονιστικές προσδοκίες σύμφωνα με το Άρθρο 32 του ΓΚΠΔ.

10.1.4 P22S – Πολιτική Καταγραφής και Παρακολούθησης: Απαιτεί την καταγραφή της χρήσης κλειδιών, των αστοχιών κρυπτογράφησης και των λήξεων πιστοποιητικών για σκοπούς ελέγχου.

10.1.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Περιγράφει λεπτομερώς τις διαδικασίες κλιμάκωσης, περιορισμού και γνωστοποίησης όταν η κρυπτογράφηση αποτυγχάνει ή όταν κλειδιά παραβιάζονται.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 8.1 – Απαιτεί την εφαρμογή λειτουργικών ελέγχων, συμπεριλαμβανομένης της κρυπτογράφησης, για τη διαχείριση κινδύνων ασφάλειας.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 8.24 – Περιγράφει απαιτήσεις για την εφαρμογή κρυπτογράφησης για τη διασφάλιση της εμπιστευτικότητας και της ακεραιότητας.

11.2.2 Έλεγχος 8.25 – Περιγράφει την ασφαλή διαχείριση κρυπτογραφικών κλειδιών και πιστοποιητικών.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-12 – Καθορίζει απαιτήσεις για τη δημιουργία και επικύρωση κρυπτογραφικών κλειδιών.

11.3.2 SC-13 – Ορίζει πρότυπα για την παραγωγή κρυπτογραφικών κλειδιών.

11.3.3 SC-17 – Καλύπτει την υποδομή δημόσιου κλειδιού (PKI) και τη διαχείριση του κύκλου ζωής των πιστοποιητικών.

11.3.4 SC-28 – Απαιτεί κρυπτογράφηση δεδομένων σε αποθήκευση.

11.3.5 SC-12 έως SC-17 (οικογένεια ελέγχων) – Διασφαλίζει ότι οι κρυπτογραφικές προστασίες υλοποιούνται ορθά σε όλα τα συστήματα.

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρο 32(1)(a) – Απαιτεί από τους οργανισμούς να εφαρμόζουν τεχνικά μέτρα, όπως η κρυπτογράφηση, για τη διασφάλιση της εμπιστευτικότητας των δεδομένων.

11.4.2 Άρθρο 34 – Ορίζει ότι η κρυπτογράφηση μπορεί να απαλλάσσει τους οργανισμούς από υποχρεώσεις γνωστοποίησης παραβίασης, εφόσον τα δεδομένα ήταν ακατανόητα για μη εξουσιοδοτημένα πρόσωπα.

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Άρθρο 21(2)(d) – Απαιτεί αποτελεσματική κρυπτογράφηση για την ασφάλεια συστημάτων και επικοινωνιών.

11.5.2 Άρθρο 21(2)(e) – Τονίζει την προστασία δεδομένων και τον μετριασμό κυβερνοαπειλών μέσω κρυπτογράφησης.

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρο 6(2)(d) – Απαιτεί τα συστήματα ΤΠΕ να διατηρούν ασφαλή κανάλια επικοινωνίας και κρυπτογράφηση.

11.6.2 Άρθρο 9(2)(f) – Υποχρεώνει τις χρηματοοικονομικές οντότητες να χρησιμοποιούν ισχυρή κρυπτογράφηση για την προστασία ψηφιακών επικοινωνιών και ανταλλαγών δεδομένων.

11.7 COBIT 2019

11.7.1 DSS05.01 – Επιβάλλει την προστασία ευαίσθητων πληροφοριών μέσω κρυπτογράφησης και κρυπτογραφικών πρωτοκόλλων.

11.7.2 APO13.02 – Απαιτεί την αποτελεσματική υλοποίηση ελέγχων ασφάλειας, συμπεριλαμβανομένων κρυπτογραφικών δικλίδων ασφαλείας, στο πλαίσιο του σχεδιασμού ασφάλειας πληροφοριών.