					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P30					Τίτλος εγγράφου: **Πολιτική αντιμετώπισης περιστατικών**							
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 8.1, Clause 9	Δομημένες διαδικασίες για τη διαχείριση κινδύνων και την αντιμετώπιση περιστατικών
ISO/IEC 27002:2022	Controls 5.25–5.27	Ρόλοι, αναφορά, αντιμετώπιση και βελτίωση για περιστατικά
NIST SP 800-53 Rev.5	IR-1 through IR-9	Ολοκληρωμένος κύκλος ζωής αντιμετώπισης περιστατικών
ΓΚΠΔ της ΕΕ	Article 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Χρονοδιαγράμματα κοινοποίησης παραβίασης, αναφορά και επικοινωνία με τα υποκείμενα των δεδομένων
Οδηγία NIS2 της ΕΕ	Article 23(1)–(4)	Κοινοποίηση στην εθνική αρμόδια αρχή και δομημένη αναφορά
Κανονισμός DORA της ΕΕ	Article 17(1)–(3)	Αναφορά μείζονος περιστατικού ΤΠΕ για χρηματοοικονομικές οντότητες
COBIT 2019	DSS02, DSS04, MEA	Καθορίζει, παρακολουθεί και αξιολογεί τη διαχείριση περιστατικών, τη συνέχεια και την αξιολόγηση

1. Σκοπός

1.1 Η παρούσα πολιτική θεσπίζει επίσημο πλαίσιο για την αναγνώριση, την αναφορά περιστατικών, την ανάλυση, τον περιορισμό, την αντιμετώπιση περιστατικών, την ανάκαμψη και την ανασκόπηση μετά το περιστατικό για περιστατικά ασφάλειας πληροφοριών που επηρεάζουν τον οργανισμό.

1.2 Διασφαλίζει έγκαιρη, συντονισμένη και αποτελεσματική αντιμετώπιση, ώστε να ελαχιστοποιούνται η επιχειρησιακή διακοπή, η οικονομική ζημία, η βλάβη στη φήμη και η κανονιστική μη συμμόρφωση.

1.3 Η πολιτική διευκολύνει επίσης τη συνεχή βελτίωση της κυβερνοανθεκτικότητας του οργανισμού μέσω των διδαγμάτων που αντλούνται και της ενσωμάτωσης των ευρημάτων μετά το περιστατικό στη διακυβέρνηση, στα εργαλεία και στα προγράμματα εκπαίδευσης.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλο το προσωπικό, συμπεριλαμβανομένων εργαζομένων, εργολάβων, συμβούλων και τρίτων παρόχων υπηρεσιών

2.1.2 Όλα τα πληροφοριακά συστήματα, τις εφαρμογές, την υποδομή, τα δίκτυα και τα δεδομένα, είτε εντός εγκαταστάσεων, είτε σε περιβάλλον νέφους, είτε σε υβριδικό περιβάλλον

2.1.3 Όλους τους τύπους περιστατικών ασφάλειας, συμπεριλαμβανομένων ενδεικτικά των εξής:

2.1.3.1 μη εξουσιοδοτημένη πρόσβαση ή κλιμάκωση δικαιωμάτων

2.1.3.2 επιθέσεις κακόβουλου λογισμικού και ransomware

2.1.3.3 επιθέσεις άρνησης υπηρεσίας (DoS/DDoS)

2.1.3.4 απώλεια, διαρροή ή εξαγωγή δεδομένων

2.1.3.5 εσωτερική κακή χρήση ή παραβιάσεις πολιτικής

2.1.3.6 παραβιάσεις φυσικής ασφάλειας που επηρεάζουν ψηφιακά περιουσιακά στοιχεία

2.2 Η πολιτική καλύπτει την ανίχνευση, την αρχική αξιολόγηση περιστατικών, τη διερεύνηση, την κλιμάκωση, τον περιορισμό, τον χειρισμό τεκμηρίων, την κοινοποίηση, την ανάκαμψη και την ανάλυση βασικής αιτίας.

3. Στόχοι

3.1 Να θεσπιστεί ικανότητα αντιμετώπισης περιστατικών που να είναι επαναλαμβανόμενη και κλιμακούμενη, επιτρέποντας την ταχεία ανίχνευση, ταξινόμηση και μετριασμό περιστατικών ασφάλειας.

3.2 Να ελαχιστοποιείται ο επιχειρησιακός αντίκτυπος των συμβάντων ασφάλειας μέσω δομημένων διαδικασιών περιορισμού, εξάλειψης και ανάκαμψης συστημάτων.

3.3 Να διασφαλίζεται ότι η αναφορά περιστατικών και η αντιμετώπιση ευθυγραμμίζονται με νομικές, κανονιστικές και συμβατικές απαιτήσεις, ιδίως όσες αφορούν τα χρονοδιαγράμματα κοινοποίησης παραβίασης και τον χειρισμό τεκμηρίων.

3.4 Να υποστηρίζεται η διαφάνεια και η λογοδοσία μέσω ορθής καταγραφής, τεκμηρίωσης και παρακολούθησης μετρικών για όλα τα περιστατικά ασφάλειας.

3.5 Να προάγεται η συνεχής βελτίωση μέσω ανασκοπήσεων μετά το περιστατικό, διορθωτικών ενεργειών και εκπαίδευσης των ενδιαφερόμενων μερών.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.1.1 Είναι υπεύθυνος για το πλαίσιο αντιμετώπισης περιστατικών, διασφαλίζει την εφαρμογή της πολιτικής και ασκεί εποπτεία στον συντονισμό περιστατικών σε επίπεδο οργανισμού.

4.1.2 Αποτελεί το κύριο σημείο επαφής με τις ρυθμιστικές αρχές, την εκτελεστική διοίκηση και τους εξωτερικούς νομικούς συμβούλους κατά τη διάρκεια μείζονων περιστατικών.

4.2 Συντονιστής Αντιμετώπισης Περιστατικών

4.2.1 Συντονίζει τις διατμηματικές ομάδες αντιμετώπισης, διαχειρίζεται τις ροές εργασίας και παρακολουθεί την κατάσταση περιορισμού και ανάκαμψης.

4.2.2 Ενεργοποιεί και συντονίζει τις ανασκοπήσεις μετά το περιστατικό (PIR) και διασφαλίζει ότι οι διορθωτικές ενέργειες καταγράφονται και υλοποιούνται.

[... 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 τουλάχιστον ετησίως και να αναθεωρείται, εφόσον απαιτείται, ώστε να ενσωματώνει:

9.1.1 Αλλαγές στο τοπίο απειλών, στους τύπους περιστατικών ή στους φορείς επίθεσης

9.1.2 Διδάγματα από μείζονα περιστατικά, παρ' ολίγον συμβάντα ή ευρήματα ρυθμιστικών αρχών

9.1.3 Επικαιροποιήσεις εφαρμοστέων νόμων και κανονισμών (π.χ. ΓΚΠΔ, DORA, NIS2)

9.1.4 Ανατροφοδότηση από ασκήσεις αντιμετώπισης περιστατικών και ανασκοπήσεις μετά το περιστατικό

9.2 Ο CISO είναι υπεύθυνος για την έναρξη και τον συντονισμό της διαδικασίας ανασκόπησης, σε διαβούλευση με:

9.2.1.1 Νομικό Σύμβουλο και DPO

9.2.1.2 SOC και Λειτουργίες Πληροφορικής

9.2.1.3 Ομάδες επιχειρησιακής συνέχειας και διαχείρισης κινδύνων

9.2.1.4 Εκτελεστική διοίκηση

9.3 Οι αλλαγές πολιτικής πρέπει να:

9.3.1 Τεκμηριώνονται σε αποθετήριο ελεγχόμενων εκδόσεων

9.3.2 Κοινοποιούνται σε όλες τις επηρεαζόμενες ομάδες και να ενσωματώνονται στην εκπαίδευση ευαισθητοποίησης

9.3.3 Επικυρώνονται μέσω επιτραπέζιων ασκήσεων ή ασκήσεων αντιμετώπισης περιστατικών σε πραγματικές συνθήκες εντός τριών μηνών από την έγκριση

9.4 Επείγουσες επικαιροποιήσεις που ενεργοποιούνται από αναδυόμενες απειλές, ευρήματα ελέγχου ή νέες νομικές υποχρεώσεις πρέπει να τίθενται άμεσα σε ισχύ και να καταγράφονται στο ιστορικό αναθεωρήσεων της πολιτικής.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική υποστηρίζεται από και διασυνδέεται με τις ακόλουθες οργανωσιακές πολιτικές:

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει την υπερκείμενη απαίτηση για λειτουργία με ετοιμότητα αντιμετώπισης περιστατικών και βάσει κινδύνου.

10.1.2 P5 – Πολιτική Διαχείρισης Αλλαγών: Διασφαλίζει ότι οι δραστηριότητες περιορισμού και ανάκαμψης που αφορούν υποδομές ή υπηρεσίες ακολουθούν επίσημες διαδικασίες.

10.1.3 P13 – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Υποστηρίζει την ταξινόμηση σοβαρότητας περιστατικών βάσει της ευαισθησίας των δεδομένων.

10.1.4 P15 – Πολιτική Αντιγράφων Ασφαλείας και Αποκατάστασης: Επιτρέπει την ανάκαμψη από ransomware ή καταστροφικές επιθέσεις με διασφάλιση της ακεραιότητας.

10.1.5 P18 – Πολιτική Κρυπτογραφικών Ελέγχων: Καθορίζει μέτρα κρυπτογράφησης που μειώνουν τον αντίκτυπο περιστατικών και τους κινδύνους έκθεσης δεδομένων.

10.1.6 P22 – Πολιτική Καταγραφής και Παρακολούθησης: Παρέχει τη βασική ορατότητα συμβάντων, τις ειδοποιήσεις και τη διατήρηση αρχείων καταγραφής που απαιτούνται για αποτελεσματική ανίχνευση και εγκληματολογική διερεύνηση.

10.1.7 P29 – Πολιτική Δεδομένων Δοκιμών και Περιβάλλοντος Δοκιμών: Διασφαλίζει ότι τα περιστατικά που επηρεάζουν συστήματα μη παραγωγικής λειτουργίας αντιμετωπίζονται επίσης με δομημένο και ασφαλή τρόπο.

10.1.8 P33 – Πολιτική Παρακολούθησης Ελέγχου και Συμμόρφωσης: Επικυρώνει την ετοιμότητα για περιστατικά και την αποτελεσματικότητα της αντιμετώπισης μέσω δομημένων ελέγχων και αξιολογήσεων συμμόρφωσης.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001: Clause 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Δομημένες διαδικασίες για τη διαχείριση κινδύνων και τον σχεδιασμό αντιμετώπισης περιστατικών.

11.2 ISO/IEC 27002:2022 – Controls 5.25–5.27: Αρμοδιότητες για τη διαχείριση περιστατικών, την αναφορά, την αντιμετώπιση, την επικοινωνία και τη βελτίωση.

11.3 NIST SP 800-53 Rev.5: IR-1 through IR-9, AU-6, PL-2: Ολοκληρωμένες απαιτήσεις για τον κύκλο ζωής αντιμετώπισης περιστατικών, τον έλεγχο και τον σχεδιασμό ασφάλειας.

11.4 ΓΚΠΔ της ΕΕ: Article 33/34: Υποχρεώσεις αναφοράς προς τις εποπτικές αρχές και απαιτήσεις ενημέρωσης των υποκειμένων των δεδομένων (με καθορισμένες εξαιρέσεις).

11.5 Οδηγία NIS2 της ΕΕ (2022/2555): Article 23: Υποχρεωτική εθνική αναφορά, με ενδιάμεσες και τελικές υποχρεώσεις αναφοράς.

11.6 Κανονισμός DORA της ΕΕ (2022/2554): Article 17: Απαιτήσεις αναφοράς περιστατικών ΤΠΕ από χρηματοπιστωτικά ιδρύματα προς τις αρμόδιες αρχές.

11.7 COBIT 2019: DSS02, DSS04, MEA01: Διαχείριση περιστατικών υπηρεσιών και συνέχειας, καθώς και παρακολούθηση απόδοσης/συμμόρφωσης.