					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P15S					Τίτλος εγγράφου: **Πολιτική Δημιουργίας Αντιγράφων Ασφαλείας και Επαναφοράς P15S**							
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	Έλεγχοι αντιγράφων ασφαλείας σύμφωνα με τις απαιτήσεις του ΣΔΑΠ
ISO/IEC 27002:2022	Έλεγχοι 5.29, 8	Βέλτιστες πρακτικές για αντίγραφα ασφαλείας, ενσωμάτωση με την επιχειρησιακή συνέχεια
NIST SP 800-53 Rev.5	CP-9, MP-6	Αντίγραφα ασφαλείας και προστασία μέσων
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(c)	Ανθεκτικότητα και συνέχεια μέσω αντιγράφων ασφαλείας
Κανονισμός DORA της ΕΕ	Άρθρο 10(1)	Συνέχεια ΤΠΕ - αντίγραφα ασφαλείας για οργανισμούς του χρηματοοικονομικού τομέα
COBIT 2019	BAI04.05, DSS04	Τεκμηρίωση και δοκιμή αντιγράφων ασφαλείας, έλεγχος διεργασιών
ΓΚΠΔ της ΕΕ	Άρθρα 5(1)(f), 32(1)(c)	Ακεραιότητα, διαθεσιμότητα και έγκαιρη αποκατάσταση δεδομένων

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τον τρόπο με τον οποίο ο οργανισμός εκτελεί και διαχειρίζεται τα αντίγραφα ασφαλείας, ώστε να διασφαλίζεται η επιχειρησιακή συνέχεια, να προστατεύεται από απώλεια δεδομένων και να καθίσταται δυνατή η έγκαιρη ανάκαμψη από περιστατικά.

1.2 Θεσπίζει δεσμευτικούς κανόνες για τον τρόπο με τον οποίο τα συστήματα και τα δεδομένα πρέπει να υποβάλλονται σε δημιουργία αντιγράφων ασφαλείας, να αποθηκεύονται και να επαναφέρονται, ιδίως σε ΜΜΕ χωρίς σύνθετη υποδομή πληροφορικής.

1.3 Η παρούσα πολιτική υποστηρίζει την ετοιμότητα για έλεγχο και την πιστοποίηση ISO/IEC 27001, διασφαλίζοντας ότι οι ουσιώδεις έλεγχοι αντιγράφων ασφαλείας εφαρμόζονται, τηρούνται με συνέπεια και ανασκοπούνται τακτικά.

1.4 Η ικανότητα του οργανισμού να ανακάμπτει από τεχνικές αστοχίες, τυχαία διαγραφή ή περιστατικά κυβερνοασφάλειας εξαρτάται από την αυστηρή τήρηση της παρούσας πολιτικής.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα επιχειρησιακά συστήματα και δεδομένα, συμπεριλαμβανομένων των εξής:

2.1.1 Οικονομικά αρχεία, πληροφορίες πελατών και δεδομένα ανθρώπινου δυναμικού

2.1.2 Επιτραπέζιοι υπολογιστές, φορητοί υπολογιστές, διακομιστές και εφαρμογές νέφους που χρησιμοποιούνται στις επιχειρησιακές λειτουργίες

2.1.3 Μέσα αντιγράφων ασφαλείας, όπως μονάδες USB, εξωτερικά μέσα αποθήκευσης ή αντίγραφα ασφαλείας σε περιβάλλον νέφους

2.2 Εφαρμόζεται επίσης σε όλα τα πρόσωπα που έχουν ευθύνη για τον χειρισμό ή τη διαχείριση διεργασιών αντιγράφων ασφαλείας, συμπεριλαμβανομένων των εξής:

2.2.1 Ο Γενικός Διευθυντής (GM) ή άλλο ορισμένο υπεύθυνο πρόσωπο

2.2.2 Εξωτερικοί πάροχοι υποστήριξης πληροφορικής ή σύμβουλοι

2.2.3 Όλοι οι εργαζόμενοι που είναι υπεύθυνοι για την αποθήκευση δεδομένων σε εγκεκριμένες τοποθεσίες

3. Στόχοι

3.1 Να διασφαλίζεται ότι όλα τα κρίσιμα επιχειρησιακά δεδομένα και συστήματα υποβάλλονται σε ασφαλή δημιουργία αντιγράφων ασφαλείας σε κατάλληλα χρονικά διαστήματα, βάσει κινδύνου και επιχειρησιακής ανάγκης.

3.2 Να διασφαλίζεται ότι τα δεδομένα μπορούν να ανακτηθούν έγκαιρα και πλήρως μετά από διαταραχές.

3.3 Να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση, η αλλοίωση ή η απώλεια δεδομένων αντιγράφων ασφαλείας μέσω αποτελεσματικών ελέγχων αποθήκευσης.

3.4 Να ανατίθενται με σαφήνεια και να εφαρμόζονται οι ρόλοι και οι αρμοδιότητες για την υλοποίηση και τις δοκιμές των διαδικασιών αντιγράφων ασφαλείας.

3.5 Να υποστηρίζεται η συμμόρφωση με το ISO/IEC 27001, τον ΓΚΠΔ της ΕΕ και άλλες κανονιστικές υποχρεώσεις μέσω δομημένων και τεκμηριωμένων πρακτικών αντιγράφων ασφαλείας.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Εγκρίνει την παρούσα πολιτική και διασφαλίζει την εφαρμογή της

4.1.2 Διαθέτει πόρους και ορίζει την ευθύνη για τις δραστηριότητες δημιουργίας αντιγράφων ασφαλείας και επαναφοράς

4.1.3 Ανασκοπεί αστοχίες αντιγράφων ασφαλείας, περιστατικά ή αποκλίσεις από την πολιτική

4.1.4 Διενεργεί τις ετήσιες ανασκοπήσεις της πολιτικής και διασφαλίζει την ετοιμότητα για έλεγχο

4.2 Εξωτερικός πάροχος υποστήριξης πληροφορικής (εφόσον εφαρμόζεται)

4.2.1 Υλοποιεί και διαχειρίζεται λύσεις αντιγράφων ασφαλείας (τοπικές ή σε περιβάλλον νέφους)

4.2.2 Παρακολουθεί την επιτυχία των αντιγράφων ασφαλείας και προγραμματίζει δοκιμές επαναφοράς

4.2.3 Αναφέρει αστοχίες και περιστατικά απευθείας στον GM

4.2.4 Διασφαλίζει την κρυπτογράφηση, τους περιορισμούς πρόσβασης και τον ορθό χειρισμό των μέσων αντιγράφων ασφαλείας

[... 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 μία φορά ετησίως από τον GM. Τα εναύσματα ενδιάμεσης ανασκόπησης περιλαμβάνουν:

9.1.1 Σημαντικές αλλαγές σε συστήματα ή μεθόδους αποθήκευσης

9.1.2 Εισαγωγή νέων πλατφορμών νέφους ή υποδομών πληροφορικής

9.1.3 Νομικές ή κανονιστικές αλλαγές που επηρεάζουν την ανάκτηση δεδομένων

9.1.4 Ευρήματα από ελέγχους ή περιστατικά

9.2 Ο GM είναι υπεύθυνος για την έναρξη της ανασκόπησης, την έγκριση αλλαγών και την κοινοποίηση των επικαιροποιήσεων.

9.3 Οι εκδόσεις της πολιτικής πρέπει να παρακολουθούνται και να αρχειοθετούνται. Οι καταργημένες εκδόσεις πρέπει να υπόκεινται σε περιορισμό πρόσβασης, ώστε να αποφεύγεται σύγχυση κατά τη διάρκεια ελέγχων ή συμβάντων επιχειρησιακής ανάκαμψης.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική ευθυγραμμίζεται και συνδέεται με τις ακόλουθες πολιτικές ΜΜΕ:

10.1.1 P14S – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Ορίζει για πόσο χρόνο πρέπει να διατηρούνται τα δεδομένα αντιγράφων ασφαλείας και πώς πρέπει να διαγράφονται με ασφάλεια.

10.1.2 P13S – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Υποστηρίζει την ιεράρχηση των δεδομένων που πρέπει να υποβάλλονται σε δημιουργία αντιγράφων ασφαλείας με βάση τα επίπεδα ταξινόμησης.

10.1.3 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Καλύπτει τις διαδικασίες όταν τα αντίγραφα ασφαλείας αποτυγχάνουν ή όταν απαιτείται ανάκτηση δεδομένων μετά από παραβίαση ή διακοπή λειτουργίας.

10.1.4 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Αναθέτει σαφή αρμοδιότητα για την εποπτεία των αντιγράφων ασφαλείας και την εφαρμογή της πολιτικής.

10.1.5 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διασφαλίζει ότι ο χειρισμός προσωπικών δεδομένων στα αντίγραφα ασφαλείας ευθυγραμμίζεται με τις νομικές απαιτήσεις και τις απαιτήσεις ιδιωτικότητας.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 8.1: Επιχειρησιακός σχεδιασμός και έλεγχος των συστημάτων αντιγράφων ασφαλείας ως μέρος του ΣΔΑΠ

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 8.13: Προδιαγράφει βέλτιστες πρακτικές για τον προγραμματισμό, την παρακολούθηση και την επαναφορά αντιγράφων ασφαλείας

11.2.2 Παράρτημα Α, Έλεγχος 5.29: Ενσωμάτωση αντιγράφων ασφαλείας με την επιχειρησιακή συνέχεια και την ετοιμότητα επαναφοράς

11.3 NIST SP 800-53 Rev.

11.3.1 CP-9 (Contingency Planning): Ορίζει δομημένες στρατηγικές αντιγράφων ασφαλείας για επιχειρησιακή ανθεκτικότητα

11.3.2 MP-6 (Media Protection): Απαιτεί ασφαλή χειρισμό και καταστροφή μέσων αντιγράφων ασφαλείας

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρο 5(1)(f): Απαιτεί ακεραιότητα και διαθεσιμότητα των προσωπικών δεδομένων

11.4.2 Άρθρο 32(1)(c): Απαιτεί τη δυνατότητα έγκαιρης αποκατάστασης της πρόσβασης σε προσωπικά δεδομένα

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Άρθρο 21(2)(c): Απαιτεί αντίγραφα ασφαλείας και ανάκαμψη ως μέρος του σχεδιασμού ανθεκτικότητας και συνέχειας

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρο 10(1): Οι οργανισμοί του χρηματοοικονομικού τομέα πρέπει να διασφαλίζουν αντίγραφα ασφαλείας ως μέρος των μέτρων συνέχειας ΤΠΕ

11.7 COBIT 2019

11.7.1 BAI04.05: Απαιτεί τεκμηριωμένες στρατηγικές αντιγράφων ασφαλείας

11.7.2 DSS04.07: Τονίζει τη σημασία των τακτικών δοκιμών και του ελέγχου των διεργασιών δημιουργίας αντιγράφων ασφαλείας και ανάκτησης δεδομένων