					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P15					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	Ρήτρες 6.1.3, 8.1	Αντιμετώπιση κινδύνων, σχεδιασμός και επιχειρησιακοί έλεγχοι αντιγράφων ασφαλείας
ISO/IEC 27002:2022	Έλεγχοι 8.13, 5.28, 5.29	Διαχείριση αντιγράφων ασφαλείας, ασφαλής διάθεση και ανθεκτικότητα
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Απαιτήσεις για αντίγραφα ασφαλείας συστημάτων, ανάκαμψη και εξυγίανση μέσων
ΓΚΠΔ της ΕΕ	Άρθρο 32, Αιτιολογική Σκέψη 49	Αποκατάσταση και διαθεσιμότητα δεδομένων προσωπικού χαρακτήρα, επιχειρησιακή συνέχεια
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(c-e)	Έλεγχοι αντιγράφων ασφαλείας και επιχειρησιακής συνέχειας για ανθεκτικότητα
Κανονισμός DORA της ΕΕ	Άρθρα 10, 11	Απαιτήσεις για αντίγραφα ασφαλείας, ανάκαμψη και δοκιμές στον χρηματοοικονομικό τομέα
COBIT 2019	DSS01, DSS04, MEA03	Λειτουργίες αντιγράφων ασφαλείας, συνέχεια και παρακολούθηση συμμόρφωσης

1. Σκοπός

1.1 Σκοπός της παρούσας πολιτικής είναι να καθορίσει τις υποχρεωτικές απαιτήσεις για τη λήψη αντιγράφων ασφαλείας και την αποκατάσταση δεδομένων, συστημάτων και εφαρμογών, με στόχο την υποστήριξη της λειτουργικής ανθεκτικότητας, της ακεραιότητας των δεδομένων και της επιχειρησιακής συνέχειας.

1.2 Η πολιτική θεσπίζει ένα τυποποιημένο πλαίσιο ώστε να:

1.2.1 Προστατεύονται τα δεδομένα του οργανισμού από απώλεια λόγω διαγραφής, αλλοίωσης, αστοχίας ή κυβερνοεπιθέσεων

1.2.2 Καθορίζονται οι απαιτήσεις ανάκαμψης μέσω σαφώς ορισμένων παραμέτρων RTO (Recovery Time Objective) και RPO (Recovery Point Objective)

1.2.3 Ενσωματώνονται οι λειτουργίες αντιγράφων ασφαλείας στο ευρύτερο ISMS και στα Σχέδια Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή (BCP/DRP)

1.2.4 Διασφαλίζεται η συμμόρφωση με την ισχύουσα νομοθεσία και τους τομεακούς κανονισμούς ως προς τη διαθεσιμότητα και τη δυνατότητα αποκατάστασης

1.3 Η πολιτική εφαρμόζει τους ελέγχους του ISO/IEC 27001:2022 που σχετίζονται με την ασφαλή διάθεση δεδομένων (5.28), την ανθεκτικότητα (5.29) και τα αντίγραφα ασφαλείας πληροφοριών (8.13), και ευθυγραμμίζεται με βέλτιστες πρακτικές των ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, ΓΚΠΔ της ΕΕ, Κανονισμού DORA της ΕΕ και Οδηγίας NIS2 της ΕΕ.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλα τα επιχειρησιακά κρίσιμα και λειτουργικά συστήματα που εμπίπτουν στο πεδίο εφαρμογής του ISMS

2.1.2 Όλα τα δομημένα και αδόμητα επιχειρησιακά δεδομένα, συμπεριλαμβανομένων βάσεων δεδομένων, αρχείων, μηνυμάτων ηλεκτρονικού ταχυδρομείου και παραμετροποιήσεων

2.1.3 Όλα τα περιβάλλοντα — εντός εγκαταστάσεων, σε περιβάλλον νέφους, υβριδικά και απομακρυσμένης/εκτός εγκαταστάσεων αποθήκευσης

2.1.4 Όλο το προσωπικό που είναι υπεύθυνο για τη διαχείριση, εκτέλεση, επαλήθευση ή αποκατάσταση διαδικασιών αντιγράφων ασφαλείας

2.2 Εφαρμόζεται επίσης σε:

2.2.1 Τα μέσα και την υποδομή αντιγράφων ασφαλείας, συμπεριλαμβανομένων φυσικών ταινιών, εικονικών συσκευών, στιγμιοτύπων δίσκου και λύσεων αντιγράφων ασφαλείας που βασίζονται σε περιβάλλον νέφους

2.2.2 Τρίτους παρόχους υπηρεσιών που έχουν συμβληθεί για τη φιλοξενία, διαχείριση ή επεξεργασία αντιγράφων ασφαλείας του οργανισμού

2.2.3 Τα αντίγραφα ασφαλείας των αρχείων καταγραφής, των παραμετροποιήσεων, των διαδρομών ελέγχου και της κρίσιμης για τη συνέχεια λειτουργικής τεκμηρίωσης

2.3 Συστήματα που εξαιρούνται ρητά από τη λήψη αντιγράφων ασφαλείας πρέπει να τεκμηριώνονται, να υποβάλλονται σε αξιολόγηση κινδύνου και να εγκρίνονται τυπικά από τον Υπεύθυνο ISMS και τον Ιδιοκτήτη Συστήματος.

3. Στόχοι

3.1 Να διασφαλίζεται ότι όλα τα κρίσιμα συστήματα και δεδομένα καλύπτονται από αξιόπιστα αντίγραφα ασφαλείας με επαρκή συχνότητα, πλεονασμό και ελέγχους ασφάλειας.

3.2 Να παρέχονται μηχανισμοί αποκατάστασης που ικανοποιούν τις καθορισμένες απαιτήσεις RTO και RPO σε ευθυγράμμιση με τις εκτιμήσεις επιχειρηματικού αντικτύπου.

3.3 Να τηρείται πλήρης τεκμηρίωση των διαδικασιών αντιγράφων ασφαλείας, των χρονοδιαγραμμάτων διατήρησης, των ρόλων και των τεχνολογιών.

3.4 Να επικυρώνεται η αποτελεσματικότητα των λειτουργιών αντιγράφων ασφαλείας μέσω συστηματικών δοκιμών αποκατάστασης, καταγραφής αστοχιών και παρακολούθησης της αποκατάστασης.

3.5 Να προστατεύονται τα δεδομένα αντιγράφων ασφαλείας από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση ή καταστροφή σε όλο τον κύκλο ζωής τους.

3.6 Να διασφαλίζεται συμμόρφωση με:

3.6.1 Τις απαιτήσεις επιχειρησιακών ελέγχων και ελέγχων συνέχειας του ISO/IEC 27001

3.6.2 Τις οικογένειες ελέγχων CP και MP του NIST SP 800-53 για αντίγραφα ασφαλείας και εξυγίανση μέσων

3.6.3 Το Άρθρο 32 και την Αιτιολογική Σκέψη 49 του ΓΚΠΔ της ΕΕ για την αποκατάσταση της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα

3.6.4 Το Άρθρο 10 του Κανονισμού DORA της ΕΕ και το Άρθρο 21 της Οδηγίας NIS2 της ΕΕ για συνέχεια και ανθεκτικότητα ΤΠΕ

3.7 Να διασφαλίζεται ότι οι υπηρεσίες αντιγράφων ασφαλείας τρίτων πληρούν τις συμβατικές και κανονιστικές υποχρεώσεις ασφάλειας, συμπεριλαμβανομένων της κρυπτογράφησης, της διάθεσης και των πρωτοκόλλων ειδοποίησης.

4. Ρόλοι και αρμοδιότητες

4.1 Ανώτατη Διοίκηση

4.1.1 Εγκρίνει την παρούσα πολιτική και διασφαλίζει ότι τα επιχειρησιακά κρίσιμα συστήματα προστατεύονται επαρκώς μέσω εγκεκριμένων πρακτικών αντιγράφων ασφαλείας και αποκατάστασης.

4.1.2 Διασφαλίζει ότι οι λειτουργίες αντιγράφων ασφαλείας διαθέτουν επαρκείς πόρους και ανασκοπούνται περιοδικά ως προς τη συμμόρφωση με τις κανονιστικές απαιτήσεις.

4.2 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.2.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και διασφαλίζει την ευθυγράμμισή της με τα ευρύτερα πλαίσια ασφάλειας πληροφοριών, διαχείρισης κινδύνων και επιχειρησιακής συνέχειας.

4.2.2 Ασκεί εποπτεία για την ενσωμάτωση των διαδικασιών αντιγράφων ασφαλείας στα BCP/DRP, στη διαχείριση περιστατικών και στον σχεδιασμό ανθεκτικότητας.

4.2.3 Ανασκοπεί εξαιρέσεις αντιγράφων ασφαλείας και αξιολογεί προτάσεις αποδοχής κινδύνου για εξαιρέσεις κρίσιμων συστημάτων.

[... 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 ή νωρίτερα, εάν αυτό απαιτηθεί από:

9.1.1 Αλλαγές στη στρατηγική επιχειρησιακής συνέχειας ή ανάκαμψης από καταστροφή

9.1.2 Νέες κανονιστικές ή νομικές υποχρεώσεις που επηρεάζουν τη συχνότητα λήψης αντιγράφων ασφαλείας ή τη διατήρηση δεδομένων

9.1.3 Αλλαγές στην αρχιτεκτονική συστημάτων, στα εργαλεία αντιγράφων ασφαλείας ή στους παρόχους υπηρεσιών

9.1.4 Σημαντικά περιστατικά ή ευρήματα ελέγχου σχετικά με απώλεια δεδομένων ή αστοχίες ανάκαμψης

9.2 Η ανασκόπηση πρέπει να συντονίζεται από τον Επικεφαλής Ασφάλειας Πληροφοριών σε συνεργασία με:

9.2.1 Υποδομές και Λειτουργίες Πληροφορικής

9.2.2 Εσωτερικό Έλεγχο

9.2.3 Υπεύθυνο Προστασίας Δεδομένων (DPO)

9.2.4 Ομάδες Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή

9.3 Τα χρονοδιαγράμματα αντιγράφων ασφαλείας, οι κατάλογοι συστημάτων που περιλαμβάνονται, η τεκμηρίωση αποκατάστασης και τα μητρώα εξαιρέσεων πρέπει να ανασκοπούνται παράλληλα ώστε να διασφαλίζεται:

9.3.1 Η ακρίβεια της κάλυψης αντιγράφων ασφαλείας για όλα τα κρίσιμα περιουσιακά στοιχεία

9.3.2 Η συμμόρφωση με τις απαιτήσεις RTO/RPO και διατήρησης

9.3.3 Η πληρότητα των αρχείων καταγραφής δοκιμών και των αναφορών περιστατικών

9.3.4 Η αποκατάσταση κενών ελέγχου που είχαν εντοπιστεί προηγουμένως

9.4 Όλες οι επικαιροποιήσεις πρέπει:

9.4.1 Να τελούν υπό έλεγχο έκδοσης και να διατηρούνται στο Μητρώο Εγγράφων ISMS

9.4.2 Να περιλαμβάνουν σύνοψη των αλλαγών και σχετική αιτιολόγηση

9.4.3 Να εγκρίνονται από την Ανώτατη Διοίκηση

9.4.4 Να κοινοποιούνται σε όλο το επηρεαζόμενο τεχνικό και επιχειρησιακό προσωπικό

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική υποστηρίζει άμεσα και αλληλεπιδρά με τα ακόλουθα συναφή έγγραφα:

10.1.1 P6 - Πολιτική Διαχείρισης Κινδύνων: Προσδιορίζει την ιεράρχηση της προστασίας αντιγράφων ασφαλείας για συστήματα και υπηρεσίες βάσει κινδύνου.

10.1.2 P12 - Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Διασφαλίζει ότι τα συστήματα που είναι επιλέξιμα για λήψη αντιγράφων ασφαλείας απογράφονται και συνδέονται με την παρακολούθηση του κύκλου ζωής και την ταξινόμηση.

10.1.3 P13 - Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Καθοδηγεί ποιες κατηγορίες δεδομένων απαιτούν αντίγραφα ασφαλείας, συμπεριλαμβανομένων μεταδεδομένων επισήμανσης για ιεράρχηση.

10.1.4 P14 - Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Συντονίζει τη διατήρηση αντιγράφων ασφαλείας με τα κανονιστικά όρια διατήρησης και την ορθή διάθεση ληγμένων μέσων.

10.1.5 P16 - Πολιτική Απόκρυψης Δεδομένων και Ψευδωνυμοποίησης: Υποστηρίζει την ελαχιστοποίηση δεδομένων κατά τη λήψη αντιγράφων ασφαλείας ευαίσθητων συνόλων δεδομένων.

10.1.6 P30 - Πολιτική Αντιμετώπισης Περιστατικών (P30): Ενεργοποιείται σε αστοχίες αντιγράφων ασφαλείας, ζητήματα αποκατάστασης ή παραβίαση αποθετηρίων δεδομένων αντιγράφων ασφαλείας.

10.2 Οι αλληλοσυνδεόμενες αυτές πολιτικές συγκροτούν ένα συνεκτικό πλαίσιο που διασφαλίζει ότι η διακυβέρνηση αντιγράφων ασφαλείας είναι ενσωματωμένη στο ευρύτερο ISMS και στη στρατηγική λειτουργικής ανθεκτικότητας του οργανισμού.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001:

11.1.1 Ρήτρα 6.1.3 - Σχέδιο Αντιμετώπισης Κινδύνων: Υποστηρίζει την ιεράρχηση αντιγράφων ασφαλείας και τον σχεδιασμό αποκατάστασης βάσει κινδύνου.

11.1.2 Ρήτρα 8.1 - Επιχειρησιακός σχεδιασμός και έλεγχος: Ενσωματώνει ελέγχους ανάκαμψης και συνέχειας ως μέρος των επιχειρησιακών δικλίδων ασφαλείας.

11.1.3 Έλεγχος Παραρτήματος Α 5.28 - Ασφαλής διάθεση ή επαναχρησιμοποίηση εξοπλισμού: Αντιμετωπίζει την ασφαλή εξυγίανση μέσων αντιγράφων ασφαλείας.

11.1.4 Έλεγχος Παραρτήματος Α 5.29 - Ασφάλεια πληροφοριών κατά τη διάρκεια διαταραχών: Διασφαλίζει δυνατότητες αποκατάστασης κατά τη διάρκεια περιστατικών ή καταστροφών.

11.1.5 Έλεγχος Παραρτήματος Α 8.13 - Αντίγραφα ασφαλείας πληροφοριών: Καλύπτεται άμεσα μέσω προγραμματισμένων, δοκιμασμένων και ασφαλών λειτουργιών αντιγράφων ασφαλείας.

11.2 ISO/IEC 27002:2022 - Έλεγχοι 8.13, 5.28, 5.29: Οι έλεγχοι αυτοί ενισχύουν την απαίτηση για τακτικά αντίγραφα ασφαλείας, επικύρωση ακεραιότητας και σχεδιασμό αποκατάστασης σε όλα τα περιβάλλοντα πληροφορικής.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - Αντίγραφα ασφαλείας συστήματος: Καθιερώνει ολοκληρωμένες διαδικασίες αντιγράφων ασφαλείας, συμπεριλαμβανομένης της αποθήκευσης εκτός εγκαταστάσεων και των δοκιμών αποκατάστασης.

11.3.2 CP-10 - Ανάκτηση και αποκατάσταση συστήματος: Απαιτεί επικυρωμένες διαδικασίες για πλήρη ή μερική αποκατάσταση, ευθυγραμμισμένες με τους στόχους ανάκαμψης.

11.3.3 MP-6 - Εξυγίανση μέσων: Διασφαλίζει τον ασφαλή χειρισμό παρωχημένων μέσων αντιγράφων ασφαλείας.

11.3.4 SI-12 - Διαδικασίες χειρισμού πληροφοριών: Ενισχύει τις αρμοδιότητες για αντίγραφα ασφαλείας και ανάκαμψη ευαίσθητων δεδομένων.

11.4 ΓΚΠΔ της ΕΕ (2016/679):

11.4.1 Άρθρο 32 - Ασφάλεια της επεξεργασίας: Επιβάλλει δυνατότητες αποκατάστασης και δικλίδες ασφαλείας διαθεσιμότητας δεδομένων, ιδίως για δεδομένα προσωπικού χαρακτήρα.

11.4.2 Αιτιολογική Σκέψη 49: Υποστηρίζει μέτρα επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή, συμπεριλαμβανομένων ασφαλών αντιγράφων ασφαλείας ως μέρους της ανθεκτικότητας του οργανισμού.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555):

11.5.1 Άρθρο 21(2)(c-e): Απαιτεί τεχνικά και οργανωτικά μέτρα, συμπεριλαμβανομένων ελέγχων αντιγράφων ασφαλείας και συνέχειας, για τη διασφάλιση της ανθεκτικότητας των υπηρεσιών.

11.6 Κανονισμός DORA της ΕΕ (2022/2554):

11.6.1 Άρθρο 10 - Επιχειρησιακή συνέχεια ΤΠΕ: Απαιτεί από τις χρηματοοικονομικές οντότητες να διαθέτουν πλήρη αντίγραφα ασφαλείας δεδομένων, δυνατότητες ανάκαμψης και σχεδιασμό συνέχειας.

11.6.2 Άρθρο 11 - Δοκιμές Σχεδίων Επιχειρησιακής Συνέχειας ΤΠΕ: Δίνει έμφαση στην επικύρωση των δυνατοτήτων ανάκαμψης μέσω τακτικών δοκιμών.

11.7 COBIT 2019:

11.7.1 DSS01 - Διαχειριζόμενες λειτουργίες: Υποστηρίζει την αξιόπιστη παροχή υπηρεσιών μέσω της προστατευμένης διαθεσιμότητας δεδομένων.

11.7.2 DSS04 - Διαχειριζόμενη συνέχεια: Ορίζει στρατηγικούς και επιχειρησιακούς ελέγχους συνέχειας, συμπεριλαμβανομένων επικυρωμένων αντιγράφων ασφαλείας.

11.7.3 MEA03 - Παρακολούθηση, αξιολόγηση και εκτίμηση συμμόρφωσης: Απαιτεί περιοδική ανασκόπηση των μέτρων συνέχειας, συμπεριλαμβανομένης της αποτελεσματικότητας των ελέγχων αντιγράφων ασφαλείας.