					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P32					Τίτλος εγγράφου: **Πολιτική Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή**							
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**

Ευθυγράμμιση με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονιστική απαίτηση	**Ρήτρα/Άρθρο**	**Σχόλιο**
ISO/IEC 27001:2022	Ρήτρα 8	
ISO/IEC 27002:2022	Έλεγχοι 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 έως CP-11	
NIST SP 800-34 Rev.1	Σχεδιασμός αντιμετώπισης εκτάκτων καταστάσεων	Πλαίσιο
ISO 22301:2019		Απαιτήσεις Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας
ΓΚΠΔ της ΕΕ	Άρθρο 32	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(f)	
Κανονισμός DORA της ΕΕ	Άρθρο 10	
COBIT 2019	DSS	

1. Σκοπός

1.1. Η παρούσα πολιτική καθορίζει τους υποχρεωτικούς ελέγχους και τις αρμοδιότητες για τη διασφάλιση της ικανότητας του οργανισμού να διατηρεί ή να αποκαθιστά κρίσιμες επιχειρησιακές λειτουργίες και τις υποστηρικτικές υπηρεσίες ΤΠΕ κατά τη διάρκεια και μετά από διαταρακτικό περιστατικό.

1.2. Στόχος της είναι η προστασία της ζωής, της λειτουργικής σταθερότητας, των νομικών υποχρεώσεων, των δεσμεύσεων προς τους πελάτες και της φήμης του οργανισμού, μέσω της ενσωμάτωσης της ανθεκτικότητας με προληπτικό σχεδιασμό και επικυρωμένες δυνατότητες ανάκαμψης.

1.3. Η παρούσα πολιτική αποτελεί τη βάση του πλαισίου Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή του οργανισμού, διασφαλίζοντας συμμόρφωση με τις ισχύουσες κανονιστικές, συμβατικές και κλαδικές απαιτήσεις.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε όλες τις οργανωτικές μονάδες, τα πληροφοριακά συστήματα, τις επιχειρησιακές διεργασίες, το προσωπικό και τις υπηρεσίες τρίτων που ταξινομούνται ως κρίσιμα ή ουσιώδη βάσει των αποτελεσμάτων της Ανάλυσης Επιχειρησιακού Αντικτύπου (BIA).

2.2. Η πολιτική καλύπτει:

2.2.1. Φυσικές και ανθρωπογενείς διαταραχές, συμπεριλαμβανομένων κυβερνοεπιθέσεων, αστοχιών υποδομών, διακοπών λειτουργίας κέντρων δεδομένων, πανδημιών και διακοπών υπηρεσιών προμηθευτών

2.2.2. Τον σχεδιασμό, τις δοκιμές και τη συνεχή βελτίωση των Σχεδίων Επιχειρησιακής Συνέχειας (BCP) και των Σχεδίων Ανάκαμψης από Καταστροφή (DRP)

2.2.3. Τους ρόλους και τις αρμοδιότητες για την απόκριση σε καταστάσεις έκτακτης ανάγκης, τον συντονισμό της ανάκαμψης και την κλιμάκωση περιστατικών

2.3. Όλο το προσωπικό με αρμοδιότητες επιχειρησιακής συνέχειας ή ανάκαμψης, συμπεριλαμβανομένων της Πληροφορικής, των ιδιοκτητών επιχειρησιακών διεργασιών, των διαχειριστών κρίσεων και των προμηθευτών, υπόκειται στις διατάξεις της παρούσας πολιτικής.

3. Στόχοι

3.1. Η διασφάλιση της συνέχειας των επιχειρησιακών λειτουργιών και υπηρεσιών μέσω προκαθορισμένων και δοκιμασμένων διαδικασιών, με ελαχιστοποίηση του λειτουργικού, του φήμης και του νομικού αντικτύπου.

3.2. Η αποκατάσταση υπηρεσιών ΤΠΕ εντός των καθορισμένων Στόχων Χρόνου Ανάκαμψης (RTO) και Στόχων Σημείου Ανάκαμψης (RPO), σε ευθυγράμμιση με τα όρια ανοχής κινδύνου του οργανισμού.

3.3. Η ανάθεση ιδιοκτησίας για τον σχεδιασμό, την εκτέλεση και τη διακυβέρνηση της επιχειρησιακής συνέχειας και της ανάκαμψης από καταστροφή σε όλο τον οργανισμό.

3.4. Η διασφάλιση ότι οι δυνατότητες επιχειρησιακής συνέχειας δοκιμάζονται, συντηρούνται και βελτιώνονται τακτικά βάσει ρεαλιστικών σεναρίων και ευρημάτων ελέγχου.

3.5. Η κάλυψη των υποχρεώσεων συμμόρφωσης στο πλαίσιο των ISO, NIST, ΓΚΠΔ, DORA και NIS2, υποστηρίζοντας τη δέουσα επιμέλεια ως προς τη λειτουργική ανθεκτικότητα και τη διαθεσιμότητα.

4. Ρόλοι και αρμοδιότητες

4.1. Ανώτατη Διοίκηση

4.1.1. Εγκρίνει την Πολιτική Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή και διασφαλίζει τη στρατηγική ευθυγράμμιση.

4.1.2. Διαθέτει προϋπολογισμό και πόρους για την υποστήριξη της επιχειρησιακής συνέχειας, της απόκρισης σε καταστάσεις έκτακτης ανάγκης και των ασκήσεων ανάκαμψης.

4.2. Υπεύθυνος Επιχειρησιακής Συνέχειας

4.2.1. Είναι υπεύθυνος για την ανάπτυξη και τη συντήρηση των Σχεδίων Επιχειρησιακής Συνέχειας (BCP) σε επίπεδο οργανισμού και για τον συντονισμό των δοκιμών συνέχειας.

4.2.2. Τηρεί το χρονοδιάγραμμα της Ανάλυσης Επιχειρησιακού Αντικτύπου (BIA), συντονίζει την εκπαίδευση και διασφαλίζει ότι η τεκμηρίωση πληροί τις απαιτήσεις συμμόρφωσης.

[... 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 Επιχειρησιακής Συνέχειας και τον Επικεφαλής Ασφάλειας Πληροφοριών (CISO), ώστε να διασφαλίζεται η ευθυγράμμιση με:

9.1.1. Αλλαγές στις επιχειρησιακές λειτουργίες, στα κρίσιμα συστήματα ή στην υποδομή

9.1.2. Διδάγματα από περιστατικά, ελέγχους, ασκήσεις επιτραπέζιων σεναρίων ή δοκιμές DR

9.1.3. Επικαιροποιημένες κανονιστικές ή συμβατικές υποχρεώσεις (π.χ. DORA, ΓΚΠΔ, απαιτήσεις πελατών για RTO/RPO)

9.1.4. Μεταβολές στη διάθεση ανάληψης κινδύνου ή στη στρατηγική επιχειρησιακής συνέχειας του οργανισμού

9.2. Οι ανασκοπήσεις πρέπει να περιλαμβάνουν:

9.2.1. Επικύρωση της καταλληλότητας των σχεδίων και των στοιχείων επικοινωνίας

9.2.2. Επανεκτίμηση των RTO, RPO και της προτεραιοποίησης ανάκαμψης

9.2.3. Αξιολόγηση της χωρητικότητας των υπηρεσιών αντιγράφων ασφαλείας και DR

9.2.4. Ανατροφοδότηση από τα ενδιαφερόμενα μέρη που εκτέλεσαν πρόσφατα σχέδια ή δοκιμές ανάκαμψης

9.3. Όλες οι αλλαγές πολιτικής πρέπει:

9.3.1. Να τελούν υπό έλεγχο εκδόσεων με τεκμηριωμένη αιτιολόγηση και έγκριση από τα ενδιαφερόμενα μέρη

9.3.2. Να κοινοποιούνται στο βασικό προσωπικό και στις ομάδες με επικαιροποιημένες αρμοδιότητες

9.3.3. Να αποτυπώνονται σε επικαιροποιημένη εκπαίδευση, υλικό ευαισθητοποίησης και λειτουργικές διαδικασίες

9.4. Πρέπει να εκδίδονται επείγουσες ενδιάμεσες επικαιροποιήσεις όταν υπάρχει σημαντική οργανωτική αλλαγή, νομική υποχρέωση ή κρίσιμο εύρημα που καθιστά τα ισχύοντα σχέδια ή την πολιτική μη εφαρμόσιμα.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική λειτουργεί συντονισμένα με τα ακόλουθα βασικά έγγραφα:

10.1.1. P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει την απαίτηση για λειτουργία με ανθεκτικότητα και βάσει κινδύνου υπό όλες τις συνθήκες.

10.1.2. P5 – Πολιτική Διαχείρισης Αλλαγών: Διασφαλίζει ότι κάθε αλλαγή ρυθμίσεων παραμέτρων ή υποδομής που σχετίζεται με την ανάκαμψη ακολουθεί τεκμηριωμένες και εγκεκριμένες ροές εργασίας.

10.1.3. P14 – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Διέπει τον κύκλο ζωής των μέσων αντιγράφων ασφαλείας και των δεδομένων που αποκαθίστανται και χρησιμοποιούνται στις λειτουργίες επιχειρησιακής συνέχειας.

10.1.4. P15 – Πολιτική Αντιγράφων Ασφαλείας και Αποκατάστασης: Ορίζει ελέγχους για τη συχνότητα των αντιγράφων ασφαλείας, την ασφάλειά τους και την επαλήθευση της αποκατάστασης.

10.1.5. P18 – Πολιτική Κρυπτογραφικών Ελέγχων: Διασφαλίζει ότι οι διαδικασίες ανάκαμψης τηρούν τα πρότυπα κρυπτογράφησης και εμπιστευτικότητας.

10.1.6. P22 – Πολιτική Καταγραφής και Παρακολούθησης: Υποστηρίζει τον εντοπισμό και την κλιμάκωση συμβάντων που επηρεάζουν την επιχειρησιακή συνέχεια.

10.1.7. P30 – Πολιτική Αντιμετώπισης Περιστατικών: Ορίζει τις διαδικασίες περιορισμού, κλιμάκωσης και ανάλυσης βασικής αιτίας σε ευθυγράμμιση με τα εναύσματα επιχειρησιακής συνέχειας.

10.1.8. P33 – Πολιτική Ελέγχου και Παρακολούθησης Συμμόρφωσης: Επικυρώνει την ακεραιότητα και την αποτελεσματικότητα των πρακτικών επιχειρησιακής συνέχειας και ανάκαμψης σε συστήματα και διεργασίες.

11. Πρότυπα και πλαίσια αναφοράς

11.1. Η παρούσα πολιτική είναι ευθυγραμμισμένη με διεθνώς αποδεκτά πρότυπα επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή, υποστηρίζοντας την ελεγκτική επάρκεια, την ανθεκτικότητα και τη νομική συμμόρφωση.

11.2. ISO/IEC 27002

11.2.1. Παράρτημα Α, Έλεγχος 5.29 – Ασφάλεια πληροφοριών κατά τη διάρκεια διαταραχών: Απαιτεί τη συνέχιση της εφαρμογής των ελέγχων ασφάλειας υπό δυσμενείς συνθήκες.

11.2.2. Παράρτημα Α, Έλεγχος 5.30 – Ετοιμότητα ΤΠΕ για επιχειρησιακή συνέχεια: Επιβάλλει την προετοιμασία, τις δοκιμές και την επικύρωση των δυνατοτήτων ανάκαμψης ΤΠΕ.

11.3. ISO 22301:2019 – Συστήματα Διαχείρισης Επιχειρησιακής Συνέχειας

11.3.1. Παρέχει το πλαίσιο για την καθιέρωση, εφαρμογή και διατήρηση πρακτικών επιχειρησιακής συνέχειας ευθυγραμμισμένων με τους στόχους του οργανισμού και τα όρια κινδύνου.

11.4. NIST SP 800-34 Rev.1 – Οδηγός Σχεδιασμού Αντιμετώπισης Εκτάκτων Καταστάσεων

11.4.1. Περιγράφει βέλτιστες πρακτικές για σχέδια αντιμετώπισης εκτάκτων καταστάσεων συστημάτων ΤΠ, συμπεριλαμβανομένων της ανάπτυξης στρατηγικής συνέχειας, της ανάλυσης αντικτύπου και των δοκιμών σχεδίων.

11.5. ΓΚΠΔ της ΕΕ (2016/679)

11.5.1. Άρθρο 32 – Ασφάλεια της επεξεργασίας: Απαιτεί ανθεκτικότητα των συστημάτων επεξεργασίας και έγκαιρη αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα μετά από περιστατικό.

11.6. Οδηγία NIS2 της ΕΕ (2022/2555)

11.6.1. Άρθρο 21(2)(f): Επιβάλλει μέτρα επιχειρησιακής συνέχειας και διαχείρισης κρίσεων για την υποστήριξη της ασφάλειας των δικτύων και πληροφοριακών συστημάτων.

11.7. Κανονισμός DORA της ΕΕ (2022/2554)

11.7.1. Άρθρο 10 – Επιχειρησιακή συνέχεια ΤΠΕ: Απαιτεί από τις χρηματοοικονομικές οντότητες να αναπτύσσουν και να δοκιμάζουν σχέδια συνέχειας ΤΠΕ, συμπεριλαμβανομένων στόχων RTO/RPO βάσει κινδύνου και δυνατοτήτων μεταγωγής σε εφεδρικό σύστημα.

11.8. COBIT 2019

11.8.1. DSS04 – Διαχείριση επιχειρησιακής συνέχειας: Καλύπτει όλες τις πτυχές του σχεδιασμού επιχειρησιακής συνέχειας, συμπεριλαμβανομένων της αναγνώρισης απειλών, της ανάλυσης αντικτύπου, της στρατηγικής ανάκαμψης και των τακτικών δοκιμών.