					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P32S					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**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρες 6.1, 6.3, 8	
ISO/IEC 27002:2022	Έλεγχοι 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
ΓΚΠΔ της ΕΕ	Άρθρα 32, 33	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(f)	
Κανονισμός DORA της ΕΕ	Άρθρο 10	
COBIT 2019	DSS04	

1. Σκοπός

1.1 Η παρούσα πολιτική διασφαλίζει ότι ο οργανισμός μπορεί να διατηρεί τη λειτουργία των επιχειρησιακών δραστηριοτήτων του και να αποκαθιστά κρίσιμες υπηρεσίες πληροφορικής κατά τη διάρκεια και μετά από διαταρακτικά συμβάντα, όπως διακοπές ρεύματος, κυβερνοεπιθέσεις, επιθέσεις ransomware ή αστοχίες συστημάτων.

1.2 Παρέχει σαφές πλαίσιο για τον σχεδιασμό επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή (BC/DR), προσαρμοσμένο στις ανάγκες ΜΜΕ χωρίς αποκλειστικές ομάδες πληροφορικής.

1.3 Η παρούσα πολιτική υποστηρίζει τη συμμόρφωση του οργανισμού με τις υποχρεωτικές απαιτήσεις των ISO/IEC 27001:2022, ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ, του Κανονισμού DORA της ΕΕ και του COBIT 2019, ενισχύοντας παράλληλα τη λειτουργική ανθεκτικότητα και την εμπιστοσύνη των πελατών.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται στα εξής:

2.1.1 Σε όλα τα επιχειρησιακά κρίσιμα συστήματα και υπηρεσίες (π.χ. ηλεκτρονικό ταχυδρομείο, αποθήκευση σε περιβάλλον νέφους, πλατφόρμες τιμολόγησης, αρχεία πελατών)

2.1.2 Σε όλους τους εργαζομένους και τους εξωτερικούς παρόχους υπηρεσιών πληροφορικής που είναι υπεύθυνοι για την ετοιμότητα και την εκτέλεση του BC/DR

2.1.3 Σε όλους τους τύπους διαταραχών, συμπεριλαμβανομένων κυβερνοπεριστατικών, αστοχιών υλικού, απώλειας ηλεκτρικής ισχύος, πλημμύρας και αδυναμίας πρόσβασης στα γραφεία

2.2 Καλύπτει τα εξής:

2.2.1 διαχείριση αντιγράφων ασφαλείας

2.2.2 σχεδιασμό επιχειρησιακής συνέχειας (BCP)

2.2.3 λειτουργίες ανάκαμψης από καταστροφή

2.2.4 εκπαίδευση προσωπικού και δοκιμές

2.2.5 διαδικασίες νομικής και κανονιστικής απόκρισης

3. Στόχοι

3.1 Να προστατεύεται η ικανότητα του οργανισμού να παρέχει βασικές υπηρεσίες παρά τις μη προγραμματισμένες διαταραχές.

3.2 Να διασφαλίζεται η έγκαιρη αποκατάσταση συστημάτων και δεδομένων σύμφωνα με προκαθορισμένους Στόχους Χρόνου Ανάκαμψης (RTO).

3.3 Να διασφαλίζεται ότι όλο το προσωπικό ακολουθεί τις διαδικασίες συνέχειας κατά τη διάρκεια κρίσεων, με ελάχιστη σύγχυση.

3.4 Να διατηρείται η συμμόρφωση με τη νομοθεσία για την προστασία δεδομένων και τη λειτουργική ανθεκτικότητα, συμπεριλαμβανομένου του Άρθρου 32 του ΓΚΠΔ της ΕΕ και του Άρθρου 21 της Οδηγίας NIS2 της ΕΕ.

3.5 Να θεσπίζεται πρακτική και επαληθεύσιμη στρατηγική συνέχειας και ανάκαμψης κατάλληλη για ΜΜΕ.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Έχει την ευθύνη της διαδικασίας BC/DR και της παρούσας πολιτικής

4.1.2 Εγκρίνει το Σχέδιο Επιχειρησιακής Συνέχειας (BCP)

4.1.3 Συντονίζει την απόκριση σε περιστατικά και την εσωτερική επικοινωνία κατά τη διάρκεια διαταραχών

4.1.4 Πραγματοποιεί τις απαιτούμενες κανονιστικές γνωστοποιήσεις (π.χ. γνωστοποιήσεις παραβίασης κατά τον ΓΚΠΔ της ΕΕ)

4.2 Εξωτερικός Πάροχος Υπηρεσιών Πληροφορικής / Διαχειριστής Συστημάτων

4.2.1 Διατηρεί και δοκιμάζει τα αντίγραφα ασφαλείας

4.2.2 Εκτελεί τις διαδικασίες ανάκαμψης από καταστροφή όταν αυτές ενεργοποιούνται

4.2.3 Τεκμηριώνει όλες τις ενέργειες ανάκαμψης και τα συμβάντα αποκατάστασης συστημάτων

4.2.4 Αναφέρει άμεσα στον GM κρίσιμα περιστατικά πληροφορικής

[... 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 πολιτικής και σχεδίου

9.1.1 Ο Γενικός Διευθυντής (GM) πρέπει να διασφαλίζει ότι η παρούσα πολιτική και το σχετικό Σχέδιο Επιχειρησιακής Συνέχειας (BCP) ανασκοπούνται επίσημα τουλάχιστον μία φορά ετησίως.

9.1.2 Η ανασκόπηση πρέπει να περιλαμβάνει:

9.1.2.1 αξιολόγηση νέων ή αναδυόμενων κινδύνων

9.1.2.2 εκ νέου επικύρωση των RTO/RPO

9.1.2.3 επαλήθευση των πληροφοριών προμηθευτών και των στοιχείων επικοινωνίας

9.1.2.4 ευθυγράμμιση με μεταβολές στα πληροφοριακά συστήματα, στις νομικές υποχρεώσεις ή στις λειτουργίες

9.2 Επικαιροποιήσεις βάσει ενεργοποιητικών συνθηκών

9.2.1 Η παρούσα πολιτική πρέπει επίσης να επικαιροποιείται σε απόκριση στα εξής:

9.2.1.1 σημαντικά περιστατικά ή διαταραχές, ιδίως εάν οι στόχοι δεν επιτεύχθηκαν

9.2.1.2 νέες νομικές ή κανονιστικές υποχρεώσεις (π.χ. τροποποιήσεις του Κανονισμού DORA της ΕΕ)

9.2.1.3 μεταβολές σε κρίσιμα συστήματα, πλατφόρμες νέφους ή προσωπικό

9.2.1.4 ευρήματα από τις ετήσιες δοκιμές BCP/DR

9.3 Διαδικασία ελέγχου αλλαγών

9.3.1 Όλες οι αλλαγές πρέπει να εγκρίνονται από τον GM

9.3.2 Πρέπει να τηρείται αρχείο ιστορικού εκδόσεων, το οποίο να περιλαμβάνει ημερομηνία, περιγραφή της αλλαγής και τον εγκρίνοντα

9.3.3 Η επικαιροποιημένη πολιτική πρέπει να αναδιανέμεται σε όλο το σχετικό προσωπικό, συμπεριλαμβανομένου του εξωτερικού παρόχου υπηρεσιών πληροφορικής και των επικεφαλής τμημάτων

9.4 Τεκμηρίωση διδαγμάτων που αντλήθηκαν

9.4.1 Μετά από δοκιμές ή πραγματικές διαταραχές, τα τεκμηριωμένα διδάγματα που αντλήθηκαν πρέπει να ενσωματώνονται σε μελλοντικές αναθεωρήσεις

9.4.2 Οι ανασκοπήσεις αυτές πρέπει επίσης να περιλαμβάνουν αξιολογήσεις απόδοσης προμηθευτών και ελέγχους επάρκειας της απόκρισης

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική είναι στενά συνδεδεμένη με τις ακόλουθες πολιτικές SME:

10.1.1 P1S – Πολιτική Ασφάλειας Πληροφοριών: Ορίζει τους υψηλού επιπέδου στόχους ασφάλειας που πρέπει να υποστηρίζονται από τις πρακτικές συνέχειας και ανάκαμψης.

10.1.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Επιτρέπει την επείγουσα ανάκληση πρόσβασης ή την αποκατάσταση πρόσβασης χρηστών σε σενάρια επιχειρησιακής διαταραχής.

10.1.3 P6S – Πολιτική Διαχείρισης Κινδύνων: Αποτελεί τη βάση για τον εντοπισμό, την αξιολόγηση και την ιεράρχηση κινδύνων που σχετίζονται με την επιχειρησιακή συνέχεια.

10.1.4 P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Διασφαλίζει ότι οι εργαζόμενοι είναι προετοιμασμένοι να ενεργούν κατά τη διάρκεια διαταραχών και κατανοούν το BCP.

10.1.5 P15S – Πολιτική Αντιγράφων Ασφαλείας και Αποκατάστασης: Παρέχει ειδικές τεχνικές διαδικασίες για τη διασφάλιση της διαθεσιμότητας των δεδομένων και της ανάκαμψης.

10.1.6 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διασφαλίζει ότι ο σχεδιασμός επιχειρησιακής συνέχειας σέβεται την προστασία δεδομένων προσωπικού χαρακτήρα και συμμορφώνεται με τον ΓΚΠΔ της ΕΕ κατά τη διάρκεια και μετά από περιστατικά.

10.1.7 P22S – Πολιτική Καταγραφής και Παρακολούθησης: Υποστηρίζει την ανίχνευση συμβάντων που μπορεί να ενεργοποιήσουν διαδικασίες BC/DR και παρέχει ψηφιακά πειστήρια μετά από διαταραχές.

10.1.8 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Προηγείται άμεσα της ενεργοποίησης της διαδικασίας ανάκαμψης σε περίπτωση κυβερνοπεριστατικών ή επιχειρησιακών περιστατικών.

10.1.9 P31S – Πολιτική Συλλογής Τεκμηρίων και Ψηφιακής Διερεύνησης: Διασφαλίζει ότι συλλέγονται ψηφιακά πειστήρια κατά τη διάρκεια σεναρίων επιχειρησιακής συνέχειας για ανάγκες συμμόρφωσης, ασφάλισης ή διερεύνησης.

10.2 Οι πολιτικές αυτές συγκροτούν ένα συνεκτικό, ελέγξιμο πλαίσιο για ανθεκτικότητα, λογοδοσία και συνέχεια ελέγχων σε όλες τις λειτουργίες της SME.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001:

11.1.1 Ρήτρα 6.1 – Απαιτεί σχεδιασμό και αντιμετώπιση βάσει κινδύνου, συμπεριλαμβανομένων της επιχειρησιακής συνέχειας και της ανάκαμψης.

11.1.2 Ρήτρα 6.3 – Δίνει έμφαση στη συνεχή βελτίωση μετά από διαταραχές.

11.1.3 Ρήτρα 8.1 – Επιβάλλει επιχειρησιακούς ελέγχους, οι οποίοι περιλαμβάνουν τεκμηριωμένα μέτρα επιχειρησιακής συνέχειας.

11.2 ISO/IEC 27002:

11.2.1 Έλεγχος 5.29 – Απαιτεί τη θέσπιση και διατήρηση ρυθμίσεων επιχειρησιακής συνέχειας.

11.2.2 Έλεγχος 5.30 – Απαιτεί δοκιμές και ανασκόπηση των ρυθμίσεων αυτών.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – Ορίζει απαιτήσεις για σχεδιασμό εφεδρικής λειτουργίας.

11.3.2 CP-4 – Επιβάλλει εκπαίδευση εφεδρικής λειτουργίας για το προσωπικό του οργανισμού.

11.3.3 CP-6 – Καλύπτει απαιτήσεις για εναλλακτικό χώρο αποθήκευσης.

11.3.4 CP-7 – Καθορίζει απαιτήσεις για εναλλακτικό χώρο επεξεργασίας.

11.4 ΓΚΠΔ της ΕΕ:

11.4.1 Άρθρο 32 – Απαιτεί μέτρα που διασφαλίζουν τη συνεχή διαθεσιμότητα και ανθεκτικότητα των συστημάτων και υπηρεσιών επεξεργασίας.

11.4.2 Άρθρο 33 – Ενεργοποιεί υποχρεώσεις γνωστοποίησης παραβίασης όταν η αστοχία επιχειρησιακής συνέχειας έχει ως αποτέλεσμα τον συμβιβασμό δεδομένων προσωπικού χαρακτήρα.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555):

11.5.1 Άρθρο 21(2)(f) – Απαιτεί δυνατότητες σχεδιασμού επιχειρησιακής συνέχειας και διαχείρισης κρίσεων ως προϋπόθεση ετοιμότητας έναντι κυβερνοκινδύνων.

11.6 Κανονισμός DORA της ΕΕ (2022/2554):

11.6.1 Άρθρο 10 – Επιβάλλει την εφαρμογή δοκιμών ψηφιακής λειτουργικής ανθεκτικότητας και δυνατοτήτων ανάκαμψης, ιδίως για ΜΜΕ του χρηματοοικονομικού τομέα.

11.7 COBIT 2019:

11.7.1 DSS04 – Διαχείριση της συνέχειας: Παρέχει καθοδήγηση εταιρικής διακυβέρνησης για τη διατήρηση και επικύρωση της λειτουργικής ανθεκτικότητας, συμπεριλαμβανομένων της υπευθυνότητας, των δοκιμών, της ενσωμάτωσης προμηθευτών και των ανασκοπήσεων μετά από συμβάντα.