Όνομα Οργανισμού

Πολιτική Επιχειρησιακής Συνέχειας

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Επιχειρησιακής Συνέχειας |
| **Δημιουργός:** |  |
| **Έκδοση:** | 1.0 |
| **Ημερομηνία Έκδοσης:** | ηη/μμ/χχχχ |
| **Εμπιστευτικότητα:** |  |
| **Ιδιοκτήτης:** |  |

Διανομή

| Ρόλος | Όνομα | Οργανισμός | Τοποθεσία | Αριθμός Αντιτύπων |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Καταγραφή Τροποποιήσεων

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Κατάσταση Έκδοσης | Έκδοση | Ημερομηνία | Ενέργειες από | Περιγραφή |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Αναφορές

|  |  |  |
| --- | --- | --- |
| **Αρ.** |  | **Αναφορά Εγγράφου** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Υποστηρικτικό Υλικό

|  |  |
| --- | --- |
| **Αρ.** | **Αναφορά** |
| 1 |  |
| 2 |  |
| 3 |  |

Ειδικό Λεξιλόγιο

Οι όροι και συντμήσεις ορίζονται πιο κάτω:

| Όροι και συντμήσεις | Περιγραφή |
| --- | --- |
|  |  |
|  |  |
|  |  |

Πίνακας Περιεχομένων

[1. Εισαγωγή 4](#_Toc188536571)

[1.1. Σκοπός 4](#_Toc188536572)

[1.2. Πεδίο Εφαρμογής 4](#_Toc188536573)

[2. Πολιτική Επιχειρησιακής Συνέχειας 5](#_Toc188536574)

[2.1. Ανάλυση επιχειρησιακών επιπτώσεων 5](#_Toc188536575)

[2.2. Σχέδιο επιχειρησιακής συνέχειας (Business Continuity Plan) 6](#_Toc188536576)

[2.3. Ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας 8](#_Toc188536577)

[2.4. Σχέδιο αποκατάστασης από καταστροφή (Disaster Recovery Plan) 8](#_Toc188536578)

[2.5. Εφεδρικά αντίγραφα και ανάκτηση δεδομένων 10](#_Toc188536579)

[2.6. Διδάγματα και συνεχής βελτίωση 10](#_Toc188536580)

[2.7. Διαχείριση διαθεσιμότητας(Availability) 10](#_Toc188536581)

[2.8. Διαχείριση χωρητικότητας(Capacity) 11](#_Toc188536582)

[3. Αναθεώρηση 13](#_Toc188536583)

[4. Αναφορές 14](#_Toc188536584)

# Εισαγωγή

# Σκοπός

Η Πολιτική Επιχειρησιακής Συνέχειας θεσπίζει το πλαίσιο για να διασφαλίσει ότι ο [Όνομα Οργανισμού] μπορεί να διατηρήσει ή να επαναφέρει γρήγορα κρίσιμες λειτουργίες κατά τη διάρκεια και μετά από ένα γεγονός που οδήγησε σε διακοπή εργασιών, όπως μια κυβερνοεπίθεση, μια φυσική καταστροφή ή μια βλάβη συστήματος. Αποσκοπεί στην ελαχιστοποίηση των επιπτώσεων των διαταραχών στις λειτουργίες, στη διασφάλιση των βασικών πόρων και στη διασφάλιση της συνέχειας των υπηρεσιών προς τους ενδιαφερόμενους, τους πελάτες και τους πελάτες. Η πολιτική καταδεικνύει τη δέσμευση του [Όνομα Οργανισμού] για ανθεκτικότητα και λειτουργική αξιοπιστία.

Πιο συγκεκριμένα οι στόχοι της Πολιτικής Επιχειρησιακής Συνέχειας είναι:

* Ο προσδιορισμός και ιεράρχηση των κρίσιμων επιχειρηματικών διαδικασιών, πόρων και συστημάτων που απαιτούνται για τη συνέχιση της λειτουργίας του [Όνομα Οργανισμού].
* Η ανάπτυξη και διατήρηση ενός σχεδίου επιχειρησιακής συνέχειας (BCP) που περιγράφει τις διαδικασίες σε λεπτομέρεια της αντιμετώπισης των διαταραχών.
* Η ανάπτυξη και διατήρηση ενός σχεδίου Σχέδιο αποκατάστασης από καταστροφή (DRP) που περιγράφει τις διαδικασίες σε λεπτομέρεια της αντιμετώπισης των διαταραχών στα συστήματα πληροφορικής.
* Ο καθορισμός ρόλων και αρμοδιοτήτων για τη διαχείριση της επιχειρησιακής συνέχειας σε ολόκληρο τον οργανισμό.
* Η διασφάλιση της ανθεκτικότητας των κρίσιμων υποδομών και πόρων μέσω μεθοδολογίας εκτίμησης κινδύνου, στρατηγικών μετριασμού και διασφάλιση εφεδρείας.
* Η διεξαγωγή τακτικών δοκιμών, εκπαίδευσης και επικαιροποίησης του σχεδίου επιχειρησιακής συνέχειας (BCP) ώστε να διασφαλίζεται η αποτελεσματικότητα του της και η ευθυγράμμισή του με τις εκάστοτε ανάγκες του [Όνομα Οργανισμού].
* Η συμμόρφωση με τους σχετικούς νόμους, κανονισμούς και πρότυπα για την επίδειξη της απαραίτητες αξιοπιστίας και επαγγελματικότητας εκ μέρους του [Όνομα Οργανισμού].

# Πεδίο Εφαρμογής

Η Πολιτική Επιχειρησιακής Συνέχειας εφαρμόζεται σε όλα τα τμήματα, τους υπαλλήλους και τους τρίτους παρόχους υπηρεσιών που εμπλέκονται στην υποστήριξη ή την παροχή κρίσιμων επιχειρηματικών λειτουργιών του [Όνομα Οργανισμού], ανεξαρτήτως γεωγραφικής τοποθεσίας που είναι απαραίτητα για την αδιάλειπτη λειτουργία του [Όνομα Οργανισμού]. Καλύπτει τους φυσικούς, τεχνικούς και διοικητικούς πόρους που είναι απαραίτητοι για τη συνέχεια, συμπεριλαμβανομένων των συστημάτων Πληροφορικής, των εγκαταστάσεων, του προσωπικού και των αλυσίδων εφοδιασμού (supply chain).

# Πολιτική Επιχειρησιακής Συνέχειας

# Ανάλυση επιχειρησιακών επιπτώσεων

Ο [Όνομα Οργανισμού] διαθέτει μια διαδικασία ανάλυσης επιχειρησιακών επιπτώσεων για τον προσδιορισμό όλων των κρίσιμων πόρων εντός του [Όνομα Οργανισμού] και την εξαγωγή αποτελεσμάτων σε σχετική αναφορά η οποία παρουσιάζεται στην διοίκηση από την οποία και εγκρίνεται σύμφωνα και με το [BCR1] της Απόφασης Κ.ΔΠ 389/2020. Η διαδικασία αυτή πρέπει να διενεργείται ετησίως και να περιλαμβάνει τα ακόλουθα:

* Τον καθορισμό κριτηρίων αξιολόγησης που σχετίζονται με το πλαίσιο του [Όνομα Οργανισμού], συμπεριλαμβανομένων των τύπων επιπτώσεων και χρονικών πλαισίων.
* Τον εντοπισμό δραστηριοτήτων που υποστηρίζουν την παροχή των προϊόντων και υπηρεσιών του [Όνομα Οργανισμού].
* Την εφαρμογή των κριτηρίων αξιολόγησης για την εκτίμηση των αναμενόμενων επιπτώσεων με την πάροδο του χρόνου από τη διακοπή αυτών των δραστηριοτήτων.
* Την εκτίμηση του χρόνου εντός του οποίου οι επιπτώσεις από τη μη επανέναρξη των δραστηριοτήτων θα γίνουν μη αποδεκτές.
* Τον καθορισμό χρονικών πλαισίων για την επανέναρξη των δραστηριοτήτων σε ελάχιστα αποδεκτά επίπεδα λειτουργικότητας εντός του προαναφερόμενου χρόνου.
* Τον προσδιορισμό των δραστηριοτήτων με προτεραιότητα.
* Τον εντοπισμό των εξαρτήσεων των δραστηριοτήτων με προτεραιότητα, συμπεριλαμβανομένων των ανθρώπινων πόρων, των πληροφοριών και δεδομένων, των κτιρίων, των χώρων εργασίας και των σχετικών υπηρεσιών κοινής ωφέλειας, του εξοπλισμού και των αναλώσιμων, των συστημάτων ICT, των μεταφορών και logistics, της χρηματοδότησης και των συνεργατών εντός της εφοδιαστικής αλυσίδας του [Όνομα Οργανισμού].

Τα αποτελέσματα της ανάλυσης επιχειρησιακών επιπτώσεων πρέπει να καταγράφονται στα πλαίσια του ενιαίου καταλόγου στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του [Όνομα Οργανισμού].

Ο [Όνομα Οργανισμού] οφείλει να ορίσει κατάλληλους ρόλους με αρμοδιότητες για την ανάλυση των επιχειρησιακών επιπτώσεων.

Ο [Όνομα Οργανισμού] πρέπει να ιεραρχεί τις λειτουργίες και τα συστήματα με βάση την αναγκαιότητα παροχής επιχειρησιακών υπηρεσιών.

Η ανάλυση των επιχειρησιακών επιπτώσεων πρέπει να πραγματοποιείται βάσει ενός συστήματος ταξινόμησης που λαμβάνει υπόψη καθορισμένα επίπεδα κρισιμότητας και εξετάζει αν οι κρίσιμες λειτουργίες ή συστήματα λειτουργούν αυτόνομα ή συνδέονται με άλλες λειτουργίες ή συστήματα του [Όνομα Οργανισμού]. Προς αυτή τη κατεύθυνση και όπου είναι δυνατό θα πρέπει να διενεργούνται συναντήσεις με αντιπροσωπευτικό μέρος του προσωπικού από κάθε εμπλεκόμενο τμήμα για τη συλλογή στοιχείων για την ανάλυση επιχειρησιακών επιπτώσεων.

Οι πιθανές στρατηγικές επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή πρέπει να αναλύονται και να καταγράφονται, ανά διεργασία, ανά είδος επίπτωσης και στην αναφορά προς τη διοίκηση πρέπει να περιλαμβάνει τουλάχιστον τα στοιχεία για τα Recovery Time Objective (RTO), Maximum Allowable Outage (MAO)/ Maximum Tolerable Period of Disruption (MTPD), Recovery Point Objective (RPO) και Minimum Business Continuity Objective (MBCO) που έχει προσδιορίσει ο [Όνομα Οργανισμού] για κάθε διαδικασία ή δραστηριότητα.

Όπου είναι δυνατό, οι στρατηγικές επιχειρησιακής συνέχειας πρέπει να καταγράφονται και να παρουσιάζονται στη διοίκηση, συνοδευόμενες από ανάλυση κόστους-οφέλους (Cost Benefit Analysis). Η διοίκηση αξιολογεί αυτές τις στρατηγικές και τις εγκρίνει ανά περίπτωση. Ακολούθως, τα σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή καταρτίζονται σύμφωνα με τις στρατηγικές που έχουν εγκριθεί από τη διοίκηση.

Οι κλίμακες που χρησιμοποιούνται για την αξιολόγηση των αναμενόμενων επιπτώσεων, καθώς και για την ανάλυση και αξιολόγηση κινδύνων, θα πρέπει να είναι εγκεκριμένες από τη διοίκηση του [Όνομα Οργανισμού] και διατυπωμένες με τέτοιο τρόπο ώστε να είναι κατανοητές από όλο το εμπλεκόμενο προσωπικό.

Η ανάλυση των επιχειρησιακών επιπτώσεων πρέπει να πραγματοποιείται τουλάχιστον σε επίπεδο:

* συμμόρφωσης του [Όνομα Οργανισμού],
* επίτευξης των στόχων του [Όνομα Οργανισμού],
* οικονομικών επιπτώσεων, επίπτωσης στη φήμη του [Όνομα Οργανισμού],
* επίπτωσης στην υγεία, ασφάλεια και ευημερία του προσωπικού,
* καθώς και επίπτωσης στην υγεία, ασφάλεια και ευημερία των χρηστών των υπηρεσιών.

# Σχέδιο επιχειρησιακής συνέχειας (Business Continuity Plan)

Το σχέδιο Επιχειρησιακής Συνέχειας αφορά την ολιστική διοικητική διαδικασία που αναγνωρίζει πιθανές απειλές για διακοπή των εργασιών του [Όνομα Οργανισμού], είτε αυτές οφείλονται σε εσωτερικούς ή εξωτερικούς παράγοντες. Για παράδειγμα: πανδημία, φυσικές καταστροφές (όπως οι καταιγίδες και οι πλημμύρες), ανθρωπογενείς καταστροφές (όπως η τρομοκρατία ή φωτιά), ή μεγαλύτερου εύρου αποτυχίες των συστημάτων πληροφορικής. Η διαχείριση της επιχειρησιακής συνέχειας των εργασιών παρέχει πλαίσιο για την οικοδόμηση οργανωτικής ανθεκτικότητας με δυνατότητα για αποτελεσματική αντίδραση, που διαφυλάσσει τα συμφέροντα των βασικών εξωτερικών συνεργατών, τη φήμη, και τις δραστηριότητες που δημιουργούν αξία.

Σύμφωνα με το [BCR2] της Απόφασης Κ.Δ.Π 389/2020 ο [Όνομα Οργανισμού], εφαρμόζεται και διατηρείται ένα σχέδιο επιχειρησιακής συνέχειας, προκειμένου να διασφαλιστεί ότι ο [Όνομα Οργανισμού] μπορεί να ανταποκρίνεται σε καταστάσεις έκτακτης ανάγκης με άμεσο και κατάλληλο τρόπο, και να είναι σε θέση να διατηρεί τις επιχειρησιακές λειτουργίες και τις κρίσιμες δραστηριότητες, ελαχιστοποιώντας τις συνέπειες και τις ζημίες που προκύπτουν από ένα περιστατικό.

Το σχέδιο επιχειρησιακής συνέχειας επικεντρώνεται στις επιπτώσεις που μπορεί να αντιμετωπίσει ο [Όνομα Οργανισμού] λόγω μιας διακοπής της ομαλής λειτουργίας της, ανεξαρτήτως των αιτίων που την προκάλεσαν.

Κάθε σχέδιο επιχειρησιακής συνέχειας πρέπει να είναι γνωστό στο εμπλεκόμενο προσωπικό και να είναι διαθέσιμο όταν το χρειάζονται.

Επιπρόσθετα το σχέδιο περιλαμβάνει και τα ακόλουθα:

* Τον σκοπό, το πεδίο εφαρμογής και τους στόχους του κάθε σχεδίου.
* Τις παραδοχές και εξαιρέσεις του σχεδίου.
* Τους ρόλους και τις αρμοδιότητες της ομάδας που θα εφαρμόσει το σχέδιο.
* Τα βήματα και λεπτομέρειες για να συνεχίσουν ή να ανακτήσουν τις επιχειρησιακές δραστηριότητες σε προκαθορισμένο επίπεδο και εντός αποδεκτού χρονικού διαστήματος. Επίσης, περιλαμβάνει την παρακολούθηση των επιπτώσεων του περιστατικού και την ανταπόκριση για τη μείωση της έκτασής του, λαμβάνοντας υπόψη την υγεία και ασφάλεια των ατόμων, τον περιορισμό της επέκτασης της διαταραχής, και τις επιπτώσεις στο περιβάλλον και την κοινωνία.
* Καθορισμός του στόχου του σημείου ανάκτησης (RPO) και του στόχου του χρόνου αποκατάστασης (RTO), ώστε να αποφεύγονται μη αποδεκτές συνέπειες για τον [Όνομα Οργανισμού]. Τα RTO, RPO θα πρέπει να καθορίζονται για κάθε διαδικασία, υπηρεσία και, αν είναι εφικτό, για κάθε σημαντική δραστηριότητα.
* Τις απαιτήσεις πόρων όπως αναγνωρίστηκαν στην ανάλυση επιχειρησιακών επιπτώσεων, για την ορθή λειτουργία των κρίσιμων διεργασιών εντός προκαθορισμένου χρονικού διαστήματος.
* Την ανάλυση των απαιτούμενων ανθρώπινων πόρων ανάλογα με τον χρόνο.
* Κάθε σχέδιο επιχειρησιακής συνέχειας πρέπει να είναι γνωστό στο εμπλεκόμενο προσωπικό και να είναι διαθέσιμο όταν το χρειάζονται.
* Τη διαδικασία και τις αρμοδιότητες για την ενημέρωση, διάγνωση, απόφαση για ενεργοποίηση και υλοποίηση του σχεδίου.
* Τις εσωτερικές και εξωτερικές αλληλεξαρτήσεις και τις προβλέψεις για τη συνέχεια του.
* Τους τρόπους και τα στοιχεία επικοινωνίας μεταξύ των ενδιαφερόμενων μερών.
* Τη σχετική τεκμηρίωση που θα τηρείται σε περίπτωση ενεργοποίησης.
* Τη διαδικασία υπαναχώρησης (standing down).
* Όπου είναι δυνατό, οι πιθανές στρατηγικές επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή πρέπει να αναλύονται και να καταγράφονται εκείνες που, ανά διεργασία, ανά είδος επίπτωσης, ανά RTO (Recovery Time Objective) και MAO (Maximum Acceptable Outage), έχουν τη δυνατότητα να επιτρέψουν στον [Όνομα Οργανισμού] να ανακάμψει τις επιχειρησιακές του δραστηριότητες εντός του προδιαγεγραμμένου αποδεκτού χρόνου.
* Οι στρατηγικές επιχειρησιακής συνέχειας πρέπει να καταγράφονται και να παρουσιάζονται στη διοίκηση, συνοδευόμενες από ανάλυση κόστους-οφέλους (Cost Benefit Analysis). Η διοίκηση πρέπει να αξιολογεί αυτές τις στρατηγικές και να τις εγκρίνει.
* Τα σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή πρέπει να καταρτίζονται σύμφωνα με τις στρατηγικές που έχουν γίνει αποδεκτές και εγκριθεί από τη διοίκηση.

# Ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας

Ο [Όνομα Οργανισμού] πρέπει να εφαρμόζει και να διατηρεί μέτρα για τον έλεγχο, την αναθεώρηση και τη βελτίωση του σχεδίου επιχειρησιακής συνέχειας μέσω ασκήσεων προσομοίωσης συμβάντων σύμφωνα με το [BCR3] της Απόφασης Κ.Δ.Π 389/2020

Οι ασκήσεις και οι προσομοιώσεις επιχειρησιακής συνέχειας πρέπει να ελέγχουν την ανταπόκριση του [Όνομα Οργανισμού] σε περιστατικά και να εντοπίζουν ευκαιρίες βελτίωσης, επιτυγχάνοντας καλύτερα αποτελέσματα με την πάροδο του χρόνου.

Ο[Όνομα Οργανισμού] πρέπει να πραγματοποιεί ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας ετησίως. Κατά την κατάρτιση του σχεδίου επιχειρησιακής συνέχειας, εξετάζεται και η αποκατάσταση από καταστροφή.

Ο [Όνομα Οργανισμού] τηρεί σχέδιο/πρόγραμμα ασκήσεων και δοκιμών το οποίο εξασφαλίζει ότι διενεργούνται ασκήσεις και δοκιμές που είναι συμβατές με τους στόχους του [Όνομα Οργανισμού] για επιχειρησιακή συνέχεια, στηρίζονται σε κατάλληλα σενάρια και στοχεύουν σε συγκεκριμένες πτυχές των σχεδίων.

Για τις ασκήσεις και τις δοκιμές τηρούνται καταγεγραμμένα πρακτικά τα οποία **αναφέρουν** το ιστορικό της δοκιμής, τους χρόνους ανά βήμα σύμφωνα με το εφαρμόσιμο σχέδιο ή μέρος του σχεδίου, και πιθανές παρατηρήσεις.

Το σχέδιο επιχειρησιακής συνέχειας πρέπει να συνδέεται με τις διαδικασίες διαχείρισης αλλαγών για να λαμβάνονται υπόψη οι συνέπειες από όποιες αλλαγές εντός του [Όνομα Οργανισμού].

# Σχέδιο αποκατάστασης από καταστροφή (Disaster Recovery Plan)

Βάσει των πιο πάνω και του [BCR4] της Απόφασης Κ.Δ.Π 389/2020, εφαρμόζεται και διατηρείται ένα σχέδιο αποκατάστασης από καταστροφή για την αποκατάσταση και ανάκτηση κρίσιμων διαδικασιών και δραστηριοτήτων, των συστημάτων πληροφορικής και των υποστηρικτικών πόρων, όπως η παροχή ηλεκτρικής ενέργειας, μετά από ένα περιστατικό, προκειμένου να διασφαλιστεί ότι ο [Όνομα Οργανισμού] ανταποκρίνεται σε καταστάσεις έκτακτης ανάγκης με άμεσο και κατάλληλο τρόπο, και να είναι σε θέση να διατηρεί τις επιχειρησιακές λειτουργίες και τις κρίσιμες δραστηριότητες, ελαχιστοποιώντας τις συνέπειες και τις ζημίες που προκύπτουν από ένα περιστατικό.

Το σχέδιο θα πρέπει να επικεντρώνεται στις επιπτώσεις που μπορεί να αντιμετωπίσει ο [Όνομα Οργανισμού] λόγω μιας διακοπής της ομαλής λειτουργίας των συστημάτων πληροφορικής, ανεξαρτήτως των αιτίων που την προκάλεσαν.

Περιλαμβάνει μεταξύ άλλων τα ακόλουθα:

* Τον σκοπό, το πεδίο εφαρμογής και τους στόχους του σχεδίου.
* Σαφείς οδηγίες για το προσωπικό πληροφορικής για έγκαιρη και αποτελεσματική αντίδραση σε περιστατικά που επηρεάζουν το περιβάλλον των συστημάτων πληροφορικής του [Όνομα Οργανισμού].
* Τους ρόλους και τις αρμοδιότητες της ομάδας που θα εφαρμόσει το σχέδιο. Το προσωπικό που εμπλέκεται στη λειτουργία του σχεδίου αποκατάστασης από καταστροφή πρέπει να είναι πλήρως ενημερωμένο σχετικά με τις αρμοδιότητες και τις υπευθυνότητες του.
* Καθορισμός των στόχων σημείου ανάκτησης (RPO) και ο στόχων χρόνου αποκατάστασης (RTO), ώστε να αποφεύγονται μη αποδεκτές συνέπειες για τον [Όνομα Οργανισμού]. Το σχέδιο καθορίζει με σαφήνεια τον στόχο σε σχέση με τον χρόνο επαναφοράς, τη μέγιστη αποδεκτή περίοδο μη λειτουργίας των συστημάτων και πόρους που απαιτούνται για την ανάκτηση.
* Το σχέδιο αποκατάστασης από καταστροφή πρέπει να περιλαμβάνει όλους τους πόρους που απαιτούνται, όπως αναγνωρίστηκαν στην ανάλυση επιχειρησιακών επιπτώσεων, για την ορθή λειτουργία των κρίσιμων διεργασιών εντός προκαθορισμένου χρονικού διαστήματος.
* Το σχέδιο αποκατάστασης από καταστροφή προβλέπει την ύπαρξη κατάλληλου αδειοδοτημένου λογισμικού για την ανάκτηση των στοιχείων από τα σχετικά αντίγραφα ασφαλείας.
* Τις παραδοχές και τυχόν εξαιρέσεις του σχεδίου.
* Πίνακα με τα στοιχεία επικοινωνίας μεταξύ των ενδιαφερόμενων μερών.
* Τη σχετική τεκμηρίωση που θα τηρείται σε περίπτωση ενεργοποίησης του σχεδίου.

Όπου είναι εφικτό, τα αρχεία εφεδρικών αντιγράφων πρέπει να κρυπτογραφούνται με την χρήση αλγορίθμων.

Οι ενημερώσεις και αλλαγές στο σχέδιο αποκατάστασης από καταστροφή πρέπει να διενεργούνται σύμφωνα με την διαδικασία διαχείρισης αλλαγών του [Όνομα Οργανισμού].

Τα σχέδια αποκατάστασης από καταστροφή πρέπει να αποθηκεύονται σε ασφαλή τοποθεσία, προστατεύονται με τα κατάλληλα μέτρα ως πληροφορία του υψηλότερου επιπέδου διαβάθμισης και εξασφαλίζεται ότι είναι διαθέσιμα σε περίπτωση καταστροφής της κύριας εγκατάστασης.

Για τις ασκήσεις και τις δοκιμές πρέπει να τηρούνται καταγεγραμμένα πρακτικά τα οποία αναφέρουν το ιστορικό της δοκιμής, τους χρόνους ανά βήμα σύμφωνα με το εφαρμόσιμο σχέδιο ή μέρος του σχεδίου, και πιθανές παρατηρήσεις.

# Εφεδρικά αντίγραφα και ανάκτηση δεδομένων

Ο [Όνομα Οργανισμός] εφαρμόζει και διατηρεί διαδικασία εφεδρικών αντιγράφων και ανάκτησης δεδομένων, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική αποκατάσταση δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος. Ο [Όνομα Οργανισμός] έχει αναγνωρίσει έναν υπεύθυνο για την λειτουργία και την τήρηση των αντιγράφων ασφαλείας.

Οι διαδικασίες εφεδρικών αντιγράφων και ανάκτησης δεδομένων πρέπει να δοκιμάζονται επαρκώς και περιοδικά, προκειμένου να διασφαλίζεται η ορθή και αξιόπιστη λειτουργία όλων των υποστηρικτικών διαδικασιών και συστημάτων.

Τα παραγωγικά συστήματα και οι υποδομές υποστήριξης που επιτρέπουν την εφεδρεία και την αποκατάσταση δεδομένων, πρέπει να είναι γεωγραφικά διαχωρισμένες.

Τα αντίγραφα ασφαλείας πρέπει να λαμβάνουν το σύνολο της πληροφορίας ή τις αλλαγές της σε ημερήσια βάση τουλάχιστον.

Η συχνότητα λήψης αντιγράφων ασφαλείας τουλάχιστον για τα κρίσιμα συστήματα πρέπει να πραγματοποιείται ανά [ΧΧ] ώρες. Έχει δημιουργηθεί ένα σχήμα διατήρησης εφεδρικών αντιγράφων σε επίπεδο ημέρας / εβδομάδας / μήνα και έτους.

# Διδάγματα και συνεχής βελτίωση

Ο [Όνομα Οργανισμού] έχει δεσμευτεί να καλλιεργήσει μια κουλτούρα συνεχούς βελτίωσης του σχεδιασμού και της εκτέλεσης της επιχειρησιακής συνέχειας. Μετά από κάθε επιχειρηματική διαταραχή, περιστατικό ή άσκηση επιχειρησιακής συνέχειας, ο αρχηγός μαζί με τα μέλη της Ομάδας Εκτέλεσης του σχεδίου επιχειρησιακής συνέχειας ή/και του σχεδίου αποκατάστασης από καταστροφές αναλαμβάνει της διεξαγωγή μίας δομημένης συνάντησης για απολογισμό της διαδικασίας και καταγραφή των διδαγμάτων που αντλήθηκαν. Ιδανικά, η συνάντηση αυτή θα πρέπει να πραγματοποιείτε εντός 24 ωρών από την ολοκλήρωση εκτέλεσης του σχεδίου. Η Ομάδα Εκτέλεσης εξετάζει διάφορα αρχεία για να διασφαλιστεί ότι αυτά αντικατοπτρίζουν τα πραγματικά γεγονότα και την πλήρη και ακριβή καταγραφή των σεναρίων του σχεδίου. Επιπρόσθετα, εντοπίζονται οι επιτυχίες, κενά που χρήζουν βελτίωσης στα σχέδια, τις διαδικασίες και τις αντιδράσεις της Ομάδας. Τα αποτελέσματα αυτών των επισκοπήσεων θα τεκμηριώνονται και θα ενσωματώνονται σε νέα έκδοση του σχεδίου επιχειρησιακής συνέχειας και στο σχέδιο αποκατάστασης από καταστροφές. Η ενσωμάτωση των διδαγμάτων, βοηθά τον [Όνομα Οργανισμού] να προσαρμόζεται συνεχώς στους εξελισσόμενους κινδύνους.

# Διαχείριση διαθεσιμότητας(Availability)

Το αρμόδιο τμήμα Τεχνολογίας του [Όνομα Οργανισμού] πρέπει να αναπτύξει μια στρατηγική διαχείρισης διαθεσιμότητας και διατηρεί μία διαδικασία διαχείρισης της διαθεσιμότητας των πόρων ανά πάσα στιγμή και η διασφάλιση ότι παρέχεται το επιθυμητό επίπεδο των επιχειρησιακών υπηρεσιών. Η διαδικασία πρέπει να καλύπτει τόσο τα τρέχοντα προβλήματα διαθεσιμότητας και επιδόσεων, όσο και μελλοντικές απαιτήσεις. Η διαθεσιμότητα πρέπει να επανεξετάζεται σε τακτική βάση.

Στα πιο πάνω πλαίσια:

* Ο [Όνομα Οργανισμού] έχει αξιολογήσει και προσδιορίσει την κρισιμότητα των πόρων του, ώστε να μπορεί να εφαρμόζει μέτρα για την εφεδρεία τους και την διαθεσιμότητα τους ανάλογα με την κρισιμότητα του κάθε πόρου. Όλα τα συστήματα πληροφορικής που σχετίζονται με κρίσιμης σημασίας πόρο ή πόρους για τον [Όνομα Οργανισμού] θα πρέπει να έχουν καθορισμένο όριο δυναμικότητας.
* Ο εξοπλισμός του [Όνομα Οργανισμού] διαθέτει εφεδρείες σε σχέση με την ενέργεια, τη χωρητικότητα, το δίκτυο και τον τρόπο διασύνδεσης, ενώ οι κρίσιμοι εξοπλισμοί πρέπει να έχουν εφεδρεία εντός του ίδιου χώρου σε ενεργή ή ανενεργή λειτουργία.
* Ο [Όνομα Οργανισμού] διατηρεί εξοπλισμό σε δευτερεύον σημείο το οποίο μπορεί να χρησιμοποιεί ώστε να ανακάμψουν κρίσιμες λειτουργίες του [Όνομα Οργανισμού] σε περίπτωση που ο εξοπλισμός στο πρωτεύον σημείο δεν είναι διαθέσιμος.
* Σε περίπτωση που κάποιο στοιχείο ενεργητικού έχει αναγνωριστεί ότι δεν είναι διαθέσιμο, το κατάλληλο προσωπικό ειδοποιείται για την διερεύνηση και την χειροκίνητη μετάβαση στο εφεδρικό σύστημα (αν απαιτείται).
* Το επίπεδο διαθεσιμότητας των στοιχείων παρακολουθείται σε συνεχή βάση ώστε να εντοπιστούν εγκαίρως περιπτώσεις μείωσης της διαθεσιμότητας.
* Έχει προβλεφθεί ώστε να υπάρχει δυνατότητα πρόσβασης και ανάκτησης των δεδομένων όπως απαιτείται από τα εφεδρικά αντίγραφα.
* Πρέπει να εφαρμόζονται λύσεις συγχρονισμού (replication) σε εναλλακτικό χώρο για τα κρίσιμα συστήματα και να γίνεται πλήρης λειτουργική δοκιμή της κατάστασης συγχρονισμού και της δυνατότητας λειτουργίας του [Όνομα Οργανισμού], ετησίως.
* Σε περίπτωση αστοχίας ή μη διαθεσιμότητας του πρωτεύοντος εξοπλισμού γίνονται αυτόματες ενέργειες για την ενεργοποίηση του δευτερεύοντος.
* Πρέπει να τηρούνται χωριστά εφεδρικά αντίγραφα και σε τρίτη ασφαλή τοποθεσία, για να μπορεί να προστατευτεί ο [Όνομα Οργανισμού] και από επιθέσεις κυβερνοεκβιασμού.
* Θα πρέπει να αποστέλλεται αμέσως τόσο στους επιχειρησιακούς ιδιοκτήτες όσο και στους διαχειριστές συστημάτων σε περίπτωση μη διαθεσιμότητας ενός ή και πολλών συστημάτων ή αν το καθορισμένο κρίσιμο όριο έχει υπερβεί.
* Συστήνεται όπως οριστούν τουλάχιστο οι ακόλουθες τρεις κατηγορίες ως καθορισμένα όρια για σκοπούς διαθεσιμότητας/χωρητικότητας (βλέπε παράγραφο 2.7 πιο κάτω):
  + **Επίπεδο προειδοποίησης**: Είναι ένα ενδεικτικό όριο σε μια μονάδα λειτουργίας IT.
  + **Επίπεδο Συναγερμού**: Έχει επιτευχθεί ένα ενδεικτικό όριο σε μια μονάδα λειτουργίας ΙΤ που υποδεικνύει ένα κρίσιμο όριο για το οποίο θα πρέπει να αναληφθεί άμεση δράση από τον αρμόδιο μηχανικό και τον ιδιοκτήτη του συστήματος.
  + **Κρίσιμο Επίπεδο**: Η επίτευξη του κρίσιμου ορίου απαιτεί τη διαδικασία αντιμετώπισης περιστατικών ασφάλειας πληροφοριών

# Διαχείριση χωρητικότητας(Capacity)

Η χρήση των υπολογιστικών πόρων (χωρητικότητα δίσκων, ποσοστό χρήσης επεξεργαστή, δυναμικότητα ταχύτητας συστημάτων κ.α.) πρέπει να παρακολουθείται, να συντονίζεται και να προγραμματίζεται κατάλληλα για να διασφαλίζεται η απαιτούμενη διαθεσιμότητα και απόδοση των συστημάτων, σύμφωνα με τις εξελισσόμενες απαιτήσεις του [Όνομα Οργανισμού] τόσο εσωτερικά και εξωτερικά (βλέπε Πολιτική Ασφάλειας Συστημάτων).

Ο [Όνομα Οργανισμού] πρέπει να έχει υιοθετήσει διαδικασία διαχείρισης της χωρητικότητας προκειμένου να διασφαλίσει τις επιδόσεις των συστημάτων πληροφορικής, περιλαμβάνοντας και έναν μηχανισμό διαχείρισης της χωρητικότητας των κρίσιμων πόρων αυτών. Επιπλέον θα πρέπει να λαμβάνεται υπόψη η αντιμετώπιση έκτακτων καταστάσεων αυξημένης ζήτηση.

Ο [Όνομα Οργανισμού] πρέπει να πραγματοποιεί παρακολούθηση των στοιχείων χωρητικότητας των Πληροφοριακών Συστημάτων ενώ για τους κρίσιμους πόρους, η παρακολούθηση πρέπει να εφαρμόζεται με αυτοματοποιημένους μηχανισμούς.

Οι ιδιοκτήτες των στοιχείων ενεργητικού, είναι υποχρεωμένοι να καθορίσουν της απαιτούμενες διαδικασίες διαχείρισης της διαθεσιμότητας προκειμένου να διασφαλίζεται ότι παρέχεται το επιθυμητό επίπεδο και απόδοση των επιχειρησιακών αναγκών των συστημάτων πληροφοριών για την υποστήριξη των συναφών επιχειρησιακών διαδικασιών και φόρτων εργασίας. Το αρμόδιο τμήμα Τεχνολογίας του [Όνομα Οργανισμού] είναι υποχρεωμένο να διασφαλίσει ότι οι απαιτήσεις αυτές πληρούνται με την κατανομή και διατήρηση των απαραίτητων πόρων, με το ελάχιστο κόστος.

Πρέπει να διενεργείται system tuning & monitoring για την εξασφάλιση της βέλτιστης δυνατής επίδοσης σε επίπεδο χωρητικότητας.

Πρόβλεψη των μελλοντικών αναγκών χωρητικότητας. Συστήνεται όπως, για τα κρίσιμα στοιχεία ενεργητικού του οργανισμού αλλά και τις βασικές λειτουργίες έχουν διεξαχθεί μελέτες για τον σχεδιασμό των κατάλληλων πόρων σε βάθος 5ετίας.

Ο σχεδιασμός των αναγκών σε χωρητικότητα πόρων πρέπει να πραγματοποιείται λαμβάνοντας υπόψη ιστορικά και πρόσφατα δεδομένα, καθώς και τις τάσεις και τα μελλοντικά σχέδια και στόχους του [Όνομα Οργανισμού].

Ο [Όνομα Οργανισμού] θα πρέπει να διεξάγει stress tests για την επιβεβαίωση της αποτελεσματικότητας των σχετικών προβλέψεων.

# Αναθεώρηση

Η πολιτική για την Επιχειρησιακή Συνέχεια θα πρέπει να επανεξετάζεται και αναθεωρείται τουλάχιστον ετησίως για να διασφαλίζεται η ευθυγράμμιση με τους τρέχοντες επιχειρηματικούς στόχους, τις διαδικασίες και τις απειλές με στόχο τη βελτίωση της αποτελεσματικότητας της. Επίσης αυτή δύναται να αναθεωρείτε μετά από ασκήσεις ή προσομοιώσεις επιχειρησιακής συνέχειας (π.χ. επιτραπέζιες ασκήσεις, ζωντανές ασκήσεις), και επανεξετάζονται τα αποτελέσματα για τον εντοπισμό αδυναμιών ή κενών και γίνεται η ενημέρωση του σχεδίου αναλόγως.

Επιπρόσθετα, η πολιτική δύναται να αναθεωρείτε σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] ή μετά από περιστατικά ασφάλειας πληροφοριών ή κανονιστικές αλλαγές.

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Επιχειρησιακή Συνέχεια Και Ανθεκτικότητα | BCR1 | Ανάλυση επιχειρησιακών επιπτώσεων | Να εξασφαλιστεί ότι ο οργανισμός έχει αναλύσει και αξιολογήσει τις κρίσιμες επιχειρηματικές διαδικασίες που πρέπει να ληφθεί υπόψη στο σχέδιο επιχειρησιακής συνέχειας, ώστε να μπορέσει ο οργανισμός να αποκαταστήσει τις επιχειρηματικές διαδικασίες σε αποδεκτό επίπεδο, το συντομότερο δυνατόν, σε περίπτωση συμβάντος ή περιστατικού. |
| Επιχειρησιακή Συνέχεια Και Ανθεκτικότητα | BCR2 | Σχέδιο επιχειρησιακής συνέχειας | Να εξασφαλιστεί ότι ο οργανισμός διαθέτει σχέδιο για τη διατήρηση της συνέχειας των κρίσιμων επιχειρηματικών διαδικασιών και την αποκατάσταση κατά τη διάρκεια συμβάντος ή περιστατικού και μετά από αυτό. |
| Επιχειρησιακή Συνέχεια Και Ανθεκτικότητα | BCR3 | Ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας | Να διασφαλιστεί ότι ο οργανισμός και τα στελέχη του γνωρίζουν τις ευθύνες τους κατά τη διάρκεια ενός συμβάντος ή περιστατικού που ενεργοποιεί το σχέδιο επιχειρησιακής συνέχειας. |
| Επιχειρησιακή Συνέχεια Και Ανθεκτικότητα | BCR4 | Σχέδιο αποκατάστασης από καταστροφή | Να εξασφαλιστεί ότι ο οργανισμός διαθέτει σχέδιο για την αποκατάσταση των συστημάτων κρίσιμων πληροφοριών σε αποδεκτό επίπεδο κατά τη διάρκεια ή μετά από περιστατικό. |
| Ασφάλεια Δεδομένων | DS3 | Εφεδρικά αντίγραφα και ανάκτηση δεδομένων | Να καταστεί δυνατή η αποκατάσταση των πληροφοριών στο πλαίσιο συμβάντων και περιστατικών ασφάλειας. |
| Διαχείριση Στοιχείων Ενεργητικού | AM4 | Διαχείριση διαθεσιμότητας | Να διασφαλιστεί η διαθεσιμότητα δικτύων και συστημάτων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρείας και συστημάτων / διαδικασιών υψηλής διαθεσιμότητας. |
| Διαχείριση Στοιχείων Ενεργητικού | AM6 | Διαχείριση χωρητικότητας | Να εξασφαλιστεί η κατάλληλη χωρητικότητα και επίδοση των υπηρεσιών των συστημάτων και διαδικασιών πληροφοριών. |
| Ασφάλεια Δικτύου | NS6 | Εφεδρεία και υψηλή διαθεσιμότητα | Να εξασφαλιστεί της η διαθεσιμότητα πληροφοριών και δικτύων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρικού εξοπλισμού, συστημάτων και συνδέσεων υψηλής διαθεσιμότητας. |