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. Στόχος Πολιτικής 4](#_Toc158631237)

[2. Διαδικασίες 4](#_Toc158631238)

[3. Ορισμοί 4](#_Toc158631239)

[4. Στόχοι Προγράμματος ‘Διαχείρισης Επιχειρησιακής Συνέχειας’ 5](#_Toc158631240)

[5. Αναθεώρηση και αξιολόγηση πολιτικής 6](#_Toc158631241)

[6. Διαχείριση Επιχειρησιακής Συνέχειας 6](#_Toc158631242)

[6.1. Πολιτική 6](#_Toc158631243)

[6.2. Ροή διαδικασίας Επιχειρησιακής Συνέχειας 7](#_Toc158631244)

[6.3. Επιχειρησιακή Συνέχεια Εργασιών και Αξιολόγηση Κινδύνου 9](#_Toc158631245)

[6.4. Ανάπτυξη Πλάνου Επιχειρησιακής Συνέχειας Εργασιών και Εφαρμογή 10](#_Toc158631246)

[6.5. Έλεγχος, Συντήρηση και Επαναξιολόγηση του Πλάνου Επιχειρησιακής Συνέχειας Εργασιών 10](#_Toc158631247)

# Στόχος Πολιτικής

Η πολιτική επιχειρησιακής συνέχειας εργασιών του [Όνομα Οργανισμού] (στο εξής θα ονομάζεται η ‘πολιτική’) παρέχει το πλαίσιο γύρω από το οποίο αναπτύχθηκε και διατηρείται η ικανότητα του Οργανισμού να διασφαλίσει την επιχειρησιακή συνέχεια στον κίνδυνο διακοπής των συστημάτων και εργασιών του [Όνομα Οργανισμού].

Ο στόχος αυτής της πολιτικής είναι να καθορίσει τις απαιτήσεις του [Όνομα Οργανισμού] για την ανάπτυξη και τη διατήρηση ενός αποτελεσματικού προγράμματος διαχείρισης της επιχειρησιακής συνέχειας των εργασιών του. Το πρόγραμμα αυτό απαιτεί μια ολοκληρωμένη προσέγγιση των επηρεαζόμενων ατόμων, σε συνάρτηση με το χώρο εργασίας και τα συστήματα.

# Διαδικασίες

Αυτή η πολιτική δεν δίνει με λεπτομέρεια σε οποιαδήποτε λειτουργική καθοδήγηση. Υπάρχει πλάνο το οποίο στηρίζει την πολιτική και παρέχει λεπτομερείς λειτουργικές κατευθυντήριες γραμμές για τα Τμήματα/Υπηρεσίες του [Όνομα Οργανισμού], ώστε να γίνεται η αναγνώριση, η μέτρηση, η παρακολούθηση, ο έλεγχος, η υποβολή εκθέσεων και η εκ νέου αξιολόγηση του κινδύνου διακοπής της επιχειρησιακής συνέχειας.

# Ορισμοί

Ο κίνδυνος της διακοπής των εργασιών και των συστημάτων είναι ο κίνδυνος απωλειών που οφείλονται στην ανεπάρκεια ή στην αποτυχία:

* του σχεδιασμού επιχειρησιακής συνέχειας.
* της δημιουργίας αντιγράφων ασφαλείας και ανάκτησης τους
* των επείγουσων διευθετήσεων
* της ασφάλειας των πληροφοριών
* της συντήρησης και αλλαγής των συστημάτων πληροφορικής
* της αναγνώρισης των σχετικών τεχνολογικών εξελίξεων και άλλων τεχνικών αιτιών των συστημάτων που σχετίζονται με τις αποτυχίες και τα λάθη.

Η διαχείριση της επιχειρησιακής συνέχειας εργασιών ασχολείται μόνο με την άμβλυνση του κινδύνου σε σχέση με τη ‘συνέχεια’, γι’ αυτό δεν περιλαμβάνει τους συνηθισμένους επιχειρηματικούς κινδύνους των συσκευών ή των προγραμμάτων, ή της ασφάλειας των πληροφοριών, εκτός εάν αυτά κλιμακωθούν και απειλήσουν διακοπή/διαταραχή του [Όνομα Οργανισμού].

Η διαχείριση της επιχειρησιακής συνέχειας εργασιών είναι μια 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 και η φωτιά), μεγαλύτερες 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.

Από τη φύση τους, είναι σπάνια τα γεγονότα που χρειάζονται την ανταπόκριση από τη διαδικασία διαχείρισης επιχειρησιακής συνέχειας εργασιών. Τα πλάνα αυτής της πολιτικής καθορίζουν τα πρότυπα και τις διαδικασίες ανάκτησης, σε περίπτωση σημαντικής διαταραχής στον [Όνομα Οργανισμού].

Ως εκ τούτου, ο κίνδυνος σε σχέση με την επιχειρησιακή συνέχεια έχει δύο κύριες συνιστώσες:

* Ετοιμότητα - ο κίνδυνος ο Οργανισμός να μην είναι έτοιμος να εφαρμόσει την κατάλληλη ανταπόκριση σε ένα περιστατικό που επηρεάζει την επιχειρησιακή συνέχεια και
* Ανταπόκριση - ο κίνδυνος του Οργανισμού να μην πετύχει το επιθυμητό αποτέλεσμα σε ένα περιστατικό το οποίο θα έχει ως συνέπεια τη μη έγκαιρη ανάκαμψη των εργασιών του [Οργανισμού] σε εύλογο χρονικό περιθώριο

Η σοβαρότητα του αντίκτυπου ενός περιστατικού θα καθορίσει την κατάλληλη ανταπόκριση στην βάση της διαχείρισης της επιχειρησιακής συνέχειας εργασιών. Ο καθορισμός των επιπτώσεων του περιστατικού γίνεται σε σχέση με:

* Τις κρίσιμες επιχειρηματικές διαδικασίες,
* την παραβίαση κανόνων,
* τη δυσφήμιση,
* την οικονομική απώλεια ή του κόστους ευκαιρίας,
* τους ανθρώπινους πόρους,
* την αποτυχία της τεχνολογίας πληροφορικής,
* τις εγκαταστάσεις και
* τους προμηθευτές.

# Στόχοι Προγράμματος ‘Διαχείρισης Επιχειρησιακής Συνέχειας’

Το πρόγραμμα αυτό στοχεύει στην επίτευξη των ακόλουθων στόχων:

* διασφάλιση της ασφάλειας και ευημερίας των υπαλλήλων και συνεργατών στην περίπτωση ενός περιστατικού που επηρεάζει την επιχειρησιακή συνέχεια των εργασιών;
* διατήρηση του πλαισίου ελέγχου του Οργανισμού;
* προγραμματισμός για τη συνέχεια και επανέναρξη των κρίσιμων δραστηριοτήτων του Οργανισμού κατόπιν ενός περιστατικού;
* έγκαιρη επαναφορά των κρίσιμων εγκαταστάσεων, συστημάτων και διαδικασιών;
* συνεχής παροχή υπηρεσιών και λήψη υπηρεσιών από κύριους εξωτερικούς συνεργάτες;
* εφαρμογή της διαχείρισης της επιχειρησιακής συνέχειας, περιλαμβανομένου ενός προγράμματος με υπευθυνότητες που να καλύπτει όλο τον Οργανισμό;
* εφαρμογή διαδικασίας με την οποία ο Οργανισμός ενημερώνεται αν οι κρίσιμοι εξωτερικοί συνεργάτες του εφαρμόζουν ένα κατάλληλο πρόγραμμα διαχείρισης επιχειρησιακής συνέχειας.

Σε περιπτώσεις κατά τις οποίες οι εξωτερικοί συνεργάτες δεν υιοθετούν τέτοιου είδους πρόγραμμα, ο [Όνομα Οργανισμού] θα πρέπει να λάβει τα αναγκαία μέτρα και προφυλάξεις για να διασφαλίσει ότι μπορεί να ολοκληρώσει τις συγκεκριμένες δραστηριότητες (στο πλαίσιο των στόχων που έχουν τεθεί σε ‘Χρόνους Ανάκτησης’) χωρίς τη διαθεσιμότητα αυτών των μερών.

Για επίτευξη των παραπάνω στόχων, τέθηκαν οι πιο κάτω προτεραιότητες:

* ασφάλεια και ευημερία των υπαλλήλων,
* διασφάλιση της συνέχειας των υπηρεσιών του [Όνομα Οργανισμού],
* διατήρηση του πλαισίου ελέγχου του Οργανισμού,
* επίτευξη των καθορισμένων ‘Στόχων Χρόνου Ανάκτησης’ για τις κρίσιμες διαδικασίες,
* την ακεραιότητα και διατήρηση όλων των πολιτικών του [Όνομα Οργανισμού], όχι μόνο αυτών που έχουν σχέση με επικινδυνότητα,
* προστασία της φήμης του Οργανισμού.

# Αναθεώρηση και αξιολόγηση πολιτικής

Ιδιοκτήτης της υφιστάμενης πολιτικής είναι ο Προϊστάμενος του Τμήματος Διοίκησης και Ανθρώπινου Δυναμικού, ο οποίος είναι υπεύθυνος για την εφαρμογή, τήρηση και αναθεώρηση της πολιτικής αυτής, σύμφωνα με τις ακόλουθες κατευθυντήριες γραμμές:

* Σημαντικές αλλαγές στον Οργανισμό
* Περιστατικά ασφάλειας πληροφοριών ή κανονιστικές αλλαγές
* Ετήσια αναθεώρηση, εφόσον προκύπτει η ανάγκη για:
  + Βελτίωση της αποτελεσματικότητας της πολιτικής
  + Ενημέρωση της για αλλαγές στην τεχνολογία.

# Διαχείριση Επιχειρησιακής Συνέχειας

# Πολιτική

Ο [Όνομα Οργανισμού] πρέπει να εφαρμόσει τα κατάλληλα πλάνα και διαδικασίες ανάκαμψης με τη μορφή ενός Σχεδίου Επιχειρησιακής Συνέχειας για να ελαχιστοποιήσει:

* τον αντίκτυπο στους στρατηγικούς, λειτουργικούς στόχους του [Όνομα Οργανισμού] και
* τη διασφάλιση της συνέχειας ή / και ταχείας ανάκτησης της απώλειας των στοιχείων ενεργητικού και των πληροφοριών σε περίπτωση μιας απροσδόκητης διακοπής ή αποτυχίας.

Το Σχέδιο Επιχειρησιακής Συνέχειας περιλαμβάνει τις διαδικασίες για την ανάκαμψη από διακοπή εργασιών, ανεξάρτητα από την αιτία. Είναι ευθύνη των Προϊσταμένων Τμημάτων και των Υπεύθυνων Υπηρεσιών του [Όνομα Οργανισμού] να βοηθήσουν στην ανάπτυξη και την υποστήριξη του υπό αναφορά πλάνου.

Η διαδικασία ανάπτυξης πλάνων για τη διαχείριση της αδιάλειπτης συνέχειας εργασιών, πρέπει να:

* αναλύει και να αξιολογεί τις επιπτώσεις στις εργασίες και τις πιθανές απειλές των επιχειρηματικών λειτουργιών και των συστημάτων πληροφοριών;
* περιλαμβάνει αξιολόγηση και εισήγηση προτάσεων στρατηγικής για τη μείωση ή τη μεταφορά του κινδύνου (συμπεριλαμβανομένων των κατάλληλων ασφαλιστικών δικλείδων, όπου αυτές είναι διαθέσιμες);
* αναπτύσσει στρατηγική, η οποία να συνάδει με τη γενική στρατηγική του Οργανισμού;
* περιλαμβάνει περιοδικούς ελέγχους, αναθεωρήσεις και φροντίζει την ενημέρωση όλων των διαδικασιών που σχετίζονται με το πλάνο διαχείρισης αδιάλειπτης συνέχειας εργασιών;
* διασφαλίζει ότι ο σχεδιασμός της επιχειρησιακής συνέχειας έχει ενσωματωθεί στις καθημερινές εργασίες του Οργανισμού.

# Ροή διαδικασίας Επιχειρησιακής Συνέχειας

Σύμφωνα με τον Κανονισμό Κ.Δ.Π. 389/2020, ο [Όνομα Οργανισμού] πρέπει να ακολουθήσει μια ροή διαδικασίας για την επιχειρησιακή της συνέχεια:

* BCR1 Ανάλυση επιχειρησιακών επιπτώσεων:

Να εξασφαλιστεί ότι ο [Όνομα Οργανισμού] έχει αναλύσει και αξιολογήσει τις κρίσιμες επιχειρηματικές διαδικασίες που πρέπει να ληφθούν υπόψη στο σχέδιο επιχειρησιακής συνέχειας, ώστε να μπορέσει ο [Όνομα Οργανισμού] να αποκαταστήσει τις επιχειρηματικές διαδικασίες σε αποδεκτό επίπεδο, το συντομότερο δυνατόν, σε περίπτωση συμβάντος ή περιστατικού. Θέσπιση, εφαρμογή και διατήρηση διαδικασίας ανάλυσης επιχειρησιακών επιπτώσεων προκειμένου να προσδιορίσει όλα τα κρίσιμα περιουσιακά στοιχεία εντός της. Η ανάλυση των επιχειρησιακών επιπτώσεων θα επιτρέψει στον [Όνομα Οργανισμού] να ιεραρχήσει τις λειτουργίες και τα συστήματα με βάση την αναγκαιότητα παροχής επιχειρησιακών υπηρεσιών. Η ανάλυση των επιχειρησιακών επιπτώσεων διενεργείται βάσει συστήματος ταξινόμησης που λαμβάνει υπόψη καθορισμένα επίπεδα κρισιμότητας και εξετάζει εάν κρίσιμες λειτουργίες ή συστήματα λειτουργούν αυτόνομα ή συνδέονται με άλλη λειτουργία ή σύστημα του [Όνομα Οργανισμού].

* BCR2 Σχέδιο επιχειρησιακής συνέχειας

Να εξασφαλιστεί ότι ο [Όνομα Οργανισμού] διαθέτει σχέδιο για τη διατήρηση της συνέχειας των κρίσιμων επιχειρηματικών διαδικασιών και την αποκατάσταση κατά τη διάρκεια συμβάντος ή περιστατικού και μετά από αυτό. Θέσπιση, εφαρμογή και διατήρηση σχεδίου επιχειρησιακής συνέχειας προκειμένου να διασφαλιστεί ότι ο [Όνομα Οργανισμού] μπορεί να ανταποκρίνεται σε καταστάσεις έκτακτης ανάγκης με άμεσο και κατάλληλο τρόπο, και είναι σε θέση να διατηρεί επιχειρηματικές λειτουργίες ελαχιστοποιώντας τις συνέπειες και τις ζημίες που προκύπτουν από ένα περιστατικό. Το σχέδιο επιχειρησιακής συνέχειας περιλαμβάνει το σχέδιο αποκατάστασης από καταστροφή, περιγράφεται στο μέτρο [BCR4] και λαμβάνει υπόψη την ανάλυση των επιχειρησιακών επιπτώσεων.

* BCR3 Ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας

Να διασφαλιστεί ότι ο [Όνομα Οργανισμού] και τα στελέχη της γνωρίζουν τις ευθύνες κατά τη διάρκεια του συμβάντος ή περιστατικού που ενεργοποιεί το σχέδιο επιχειρησιακής συνέχειας. Θέσπιση, εφαρμογή και διατήρηση μέτρων για τον έλεγχο, την αναθεώρηση και τη βελτίωση του σχεδίου επιχειρησιακής συνέχειας μέσω ασκήσεων όπου προσομοιώνονται συμβάντα και περιστατικά στον [Όνομα Οργανισμού], με σκοπό τον έλεγχο της ανταπόκρισης της σε παρόμοια συμβάντα και περιστατικά, και τη βελτίωση των διαδικασιών επιχειρησιακής συνέχειας.

Οι ασκήσεις και οι προσομοιώσεις επιχειρησιακής συνέχειας θα πρέπει να παρέχουν στον [Όνομα Οργανισμού] τη δυνατότητα να εντοπίζει ευκαιρίες βελτίωσης και να επιτυγχάνει καλύτερα αποτελέσματα με την πάροδο του χρόνου. Ο [Όνομα Οργανισμού] θα πρέπει να εξετάσει το ενδεχόμενο να συνδέσει το σχέδιο επιχειρησιακής συνέχειας με τις διαδικασίες διαχείρισης αλλαγών, περιγράφονται στο [CM1], προκειμένου να λαμβάνονται υπόψη στο σχέδιο επιχειρησιακής συνέχειας οι συνέπειες από όποιες αλλαγές εντός του [Όνομα Οργανισμού]. Αυτό σημαίνει ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα ή η αυθεντικότητα των πληροφοριών. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να επιτρέπει στον [Όνομα Οργανισμού] να αξιολογεί τους κινδύνους στο πλαίσιο αιτημάτων αλλαγών και να σχεδιάζει αλλαγές λαμβάνοντας υπόψη κατάλληλα μέτρα ασφάλειας καθώς και να περιλαμβάνει την προετοιμασία και την επαλήθευση των αλλαγών.

Επιπρόσθετα, ο [Όνομα Οργανισμού] θα πρέπει να διενεργεί ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας σε τακτά χρονικά διαστήματα, προκειμένου οι εργαζόμενοι να είσαι σε επαγρύπνηση για συμβάντα και περιστατικά που θα μπορούσαν να την βλάψουν. Κατά την κατάρτιση του σχεδίου επιχειρησιακής συνέχειας, ο [Όνομα Οργανισμού] εξετάζει και την αποκατάσταση από καταστροφή, ορίζεται στο μέτρο [BCR4].

* BCR4 Σχέδιο αποκατάστασης από καταστροφή

Να εξασφαλιστεί ότι ο [Όνομα Οργανισμού] διαθέτει σχέδιο για την αποκατάσταση των συστημάτων κρίσιμων πληροφοριών σε αποδεκτό επίπεδο κατά τη διάρκεια ή μετά από περιστατικό. Θέσπιση, εφαρμογή και διατήρηση σχεδίου αποκατάστασης από καταστροφή, προκειμένου να διασφαλίζεται η αποκατάσταση και η ανάκτηση όλων των κρίσιμων διαδικασιών των συστημάτων πληροφορικής και των υποστηρικτικών στοιχείων ενεργητικού, η παροχή ηλεκτρικής ενέργειας, μετά την ύπαρξη του περιστατικού. Το σχέδιο αποκατάστασης από καταστροφή θα πρέπει να περιλαμβάνει σαφείς οδηγίες για το προσωπικό πληροφορικής, ώστε να εξασφαλίζεται έγκαιρη και αποτελεσματική αντίδραση σε όλα τα περιστατικά που επηρεάζουν το περιβάλλον πληροφορικής του [Όνομα Οργανισμού]. Στο σχέδιο αποκατάστασης από καταστροφή θα πρέπει να καθορίζεται ο στόχος του σημείου ανάκτησης (RPO) και ο στόχος για τον χρόνο αποκατάστασης (RTO), ώστε να αποφεύγονται μη αποδεκτές συνέπειες για τον [Όνομα Οργανισμού].

* Ανασκόπηση απολογισμού και μετά το περιστατικό

Μετά την κατάργηση του IRT, ο αρχηγός της ομάδας θα πραγματοποιήσει μια απολογισμός όλων των μελών ιδανικά εντός 24 ωρών. Τα σχετικά αρχεία του συμβάντος θα εξεταστούν από το IRT για να διασφαλιστεί ότι αντικατοπτρίζουν πραγματικά γεγονότα και αντιπροσωπεύουν πλήρη και ακριβή καταγραφή του συμβάντος. Οποιαδήποτε άμεσα σχόλια ή σχόλια από την ομάδα θα καταγράφονται. Μια πιο επίσημη επανεξέταση μετά το περιστατικό θα πραγματοποιηθεί σε χρόνο που θα αποφασίσει η ανώτατη διοίκηση ανάλογα με το μέγεθος και τη φύση του συμβάντος. Ως συμβολή σε αυτήν την ανασκόπηση, ο Αρχηγός της Ομάδας θα συμπληρώσει μια αναφορά μετά το περιστατικό.

# Επιχειρησιακή Συνέχεια Εργασιών και Αξιολόγηση Κινδύνου

Είναι σημαντικό να λαμβάνεται υπόψη από τη Διεύθυνση του [Όνομα Οργανισμού] η επίδραση που μπορεί να έχουν πιθανά συμβάντα στις κρίσιμες επιχειρηματικές λειτουργίες του [Όνομα Οργανισμού]. Για τον σκοπό αυτό, αξιολογούνται οι υψίστης σημαντικότητας επιχειρηματικές δραστηριότητες του [Όνομα Οργανισμού] και η κρισιμότητα τους, η χρηματοοικονομική και η λειτουργική επίδραση τους και άλλες βασικές απαιτήσεις για πόρους. Ως εκ τούτου, διενεργείται σχετική αξιολόγηση επικινδυνότητας και ανάλυση επιχειρησιακών επιπτώσεων.

Η ανάλυση περιλαμβάνει την αναγνώριση απειλών, όπως:

* Φυσική καταστροφή,
* Φωτιά,
* Απώλεια των κρίσιμων υπηρεσιών υποδομής, όπως ενέργεια, επικοινωνία, νερό,
* Σκόπιμη ή τυχαία βλάβη στον εξοπλισμό ή τα δεδομένα,
* Απεργία η οποία διαταράσσει τη συνέχεια της εργασίας,
* Βλάβη συστημάτων,
* Παραβίαση της ασφάλειας, και
* Σκόπιμη ή τυχαία αποκάλυψη πληροφορίας επιπέδου ‘εμπιστευτικό ή άνω’.

Το πλάνο 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.

Τα αποτελέσματα της αξιολόγησης της επικινδυνότητας και της ανάλυσης των επιχειρησιακών επιπτώσεων οδηγεί στον καθορισμό μιας στρατηγικής για την επιχειρησιακή συνέχεια, καθορίζοντας την πιο αποτελεσματική και ωφέλιμη λύση ανάκαμψης του [Όνομα Οργανισμού].

# Ανάπτυξη Πλάνου Επιχειρησιακής Συνέχειας Εργασιών και Εφαρμογή

Η αξιολόγηση επικινδυνότητας και η ανάλυση των επιχειρησιακών επιπτώσεων θα πρέπει να αποτελούν τη βάση για την ανάπτυξη του πλάνου αδιάλειπτης συνέχειας εργασιών. Είναι ευθύνη της Διεύθυνσης του [Όνομα Οργανισμού] να διασφαλίσει ότι το πλάνο επιχειρησιακής συνέχειας των εργασιών θα αποκαταστήσει στον απαιτούμενο χρόνο τις επιχειρησιακές δραστηριότητες μετά από κάθε διακοπή υπηρεσιών ή καταστροφής.

Ως εκ τούτου, τα ακόλουθα στοιχεία πρέπει να περιλαμβάνονται στο σχέδιο:

* οι απαραίτητες συνθήκες ή απαιτήσεις για να επικαλεστεί το σχέδιο,
* οι λειτουργικές και εκτάκτου ανάγκης διαδικασίες για όλες τις βασικές επιχειρηματικές διεργασίες,
* οι εναλλακτικές διαδικασίες που περιγράφουν τις ενέργειες που πρέπει να διενεργηθούν για να μετακινηθούν οι βασικές επιχειρηματικές δραστηριότητες ή οι υποστηρικτικές υπηρεσίες σε εναλλακτικές προσωρινές τοποθεσίες, και να επαναφερθούν οι διεργασίες του Οργανισμού σε λειτουργία, στα απαιτούμενα χρονικά περιθώρια,
* τα περιουσιακά στοιχεία και οι πόροι που απαιτούνται για να είναι σε θέση να εκτελεστούν οι εφεδρικές και έκτακτης ανάγκης διαδικασίες,
* οι ευθύνες των ατόμων, περιγράφοντας ποιος είναι υπεύθυνος για την εκτέλεση ποιου μέρους του σχεδίου,
* διαδικασίες ανάκαμψης που περιγράφουν τις ενέργειες που πρέπει να πραγματοποιηθούν για να επιστρέψει ο Οργανισμός σε κανονική λειτουργία,
* πρόγραμμα συντήρησης που καθορίζει πώς και πότε θα ελεγχθεί το πλάνο, και τη διαδικασία διατήρησης του σχεδίου,
* δραστηριότητες εκπαίδευσης και ενημέρωσης που έχουν σχεδιαστεί για να βοηθήσουν στην κατανόηση των διεργασιών της επιχειρησιακής συνέχειας και να διασφαλίσουν ότι οι διαδικασίες εξακολουθούν να είναι αποτελεσματικές;
* διαδικασία υποβολής εκθέσεων για την ανάκτηση και δράση μετά το συμβάν.

# Έλεγχος, Συντήρηση και Επαναξιολόγηση του Πλάνου Επιχειρησιακής Συνέχειας Εργασιών

Ο Προϊστάμενος Ασφάλειας Πληροφοριών τηρεί ένα πρόγραμμα ελέγχου. Το πρόγραμμα θα δεικνύει εάν και ποιο στοιχείο του πλάνου θα ελεγχθεί για να διαπιστωθεί ότι ο χρόνος επαναφοράς αντανακλά τις προσδοκίες του [Όνομα Οργανισμού], όποτε είναι δυνατόν, καταγράφεται ο χρόνος που χρειάστηκε για την ανάκαμψη των συστημάτων. Καταγράφονται επίσης τα αποτελέσματα οποιουδήποτε ελέγχου και ενημερώνονται οι Προϊστάμενοι Τμήματος ή Υπεύθυνοι Υπηρεσίας που κρίνονται απαραίτητοι.

Ο Προϊστάμενος Ασφάλειας Πληροφοριών είναι υπεύθυνος για την τήρηση του συνολικού πλάνου επιχειρησιακής συνέχειας και για την επικοινωνία του πλάνου αυτού στο σχετικό προσωπικό εντός του [Όνομα Οργανισμού].

Οι υπάλληλοι οι οποίοι είναι υπεύθυνοι για τις σχετικές λειτουργίες, υπό την εποπτεία του Προϊσταμένου τους, θα ελέγχουν σε τακτά χρονικά διαστήματα το πλάνο επιχειρησιακής συνέχειας που τους αφορά. Ο έλεγχος μπορεί να περιλαμβάνει:

* ‘Table top’ έλεγχος (συζήτηση των διευθετήσεων ανάκαμψης χρησιμοποιώντας παραδείγματα διακοπής εργασιών).
* Ολοκληρωμένη δοκιμή
* Προσομοίωση
* Τεχνικές δοκιμές ανάκαμψης
* Έλεγχος των εγκαταστάσεων και υπηρεσιών των εξωτερικών συνεργατών

Ο Προϊστάμενος Ασφάλειας Πληροφοριών θα ενημερώνεται για τα αποτελέσματα αυτών των ελέγχων.

Οι Προϊστάμενοι Τμημάτων και Υπεύθυνοι Υπηρεσιών είναι υπεύθυνοι να βεβαιωθούν ότι τυχόν αλλαγές στο Τμήμα / Υπηρεσία τους, όπως: (i) προσωπικό, (ii) νομοθεσία, (iii) διαδικασίες, (iv) στοιχεία επικοινωνίας και (v) θέσεις, ενσωματώθηκαν στα πλάνα επιχειρησιακής συνέχειας και ότι όλοι οι χρήστες έχουν επίγνωση των πλάνων και των ευθυνών τους.