Όνομα Οργανισμού

Σχέδιο Ανάκαμψης από Καταστροφή

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Σχέδιο Ανάκαμψης από Καταστροφή |
| **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](#_Toc190846894)

[1.1 Σκοπός 4](#_Toc190846895)

[1.2 Στόχοι του Σχεδίου 4](#_Toc190846896)

[1.3 Πεδίο εφαρμογής του σχεδίου 5](#_Toc190846897)

[2 Ορισμοί 5](#_Toc190846898)

[3 Παραδοχές 6](#_Toc190846899)

[4 Προβλεπόμενο κοινό του Σχεδίου 6](#_Toc190846900)

[5 Φύλαξη Εγγράφου 7](#_Toc190846901)

[6 Ρόλοι και ευθύνες του Σχεδίου Ανάκαμψης Καταστροφών 7](#_Toc190846902)

[6.1 Επικεφαλής ομάδας σχεδίου Ανάκαμψης καταστροφών 8](#_Toc190846903)

[6.2 Επικεφαλής Τμήματος Πληροφορικής και η Ομάδα Πληροφορικής 8](#_Toc190846904)

[6.3 Υπεύθυνος επικοινωνίας 9](#_Toc190846905)

[7 Σχέδιο Ανάκαμψης καταστροφών 9](#_Toc190846906)

[7.1 Στρατηγική Ανάκαμψης καταστροφών 9](#_Toc190846907)

[7.2 Ανάλυση επιχειρηματικών επιπτώσεων (BIA) - Καθορισμός Κρίσιμων λειτουργιών 10](#_Toc190846908)

[7.3 Πίνακας κρισιμότητας Ανάκαμψης καταστροφών (DR Criticality Matrix) 11](#_Toc190846909)

[7.4 Σενάρια 12](#_Toc190846910)

[7.5 Τοποθεσία και Συνδεσιμότητα εναλλακτικού χώρου εργασίας 12](#_Toc190846911)

[7.6 Λίστα ελέγχου δραστηριοτήτων και εργασιών Ανάκαμψης καταστροφών 12](#_Toc190846912)

[8 Συντήρηση και δοκιμές του Σχεδίου 14](#_Toc190846913)

[8.1 Αναθεώρηση σχεδίων και χρονοδιάγραμμα 14](#_Toc190846914)

[8.2 Αλλαγή διαδικασίας διαχείρισης 14](#_Toc190846915)

[8.3 Δοκιμές Ανάκαμψης καταστροφών 14](#_Toc190846916)

[Παράρτημα Α – Στοιχεία επικοινωνίας της ομάδας Ομάδα Ανάκαμψης από Καταστροφές 16](#_Toc190846917)

[Παράρτημα Β – Λίστες επαφών 16](#_Toc190846918)

[Εσωτερική λίστα επαφών 16](#_Toc190846919)

[Λίστα εξωτερικών επαφών 16](#_Toc190846920)

[Άλλα Παραρτήματα κατά περίπτωση – Αναλυτική περιγραφή Σεναρίων και Playbooks όπως καταγράφεται στη παράγραφο 7.4 του παρόντος σχεδίου 16](#_Toc190846921)

# 

## Εισαγωγή

## Σκοπός

Ο σκοπός του παρόντος Σχεδίου Ανάκαμψης από καταστροφές (Disaster Recovery Plan) είναι η καθιέρωση μιας δομημένης και τεκμηριωμένης προσέγγισης για την αντιμετώπιση διαταραχών που σχετίζονται με το τομέα Πληροφορικής και Τηλεπικοινωνιών του [Όνομα Οργανισμού] εξασφαλίζοντας την έγκαιρη ανάκαμψη κρίσιμων συστημάτων, εφαρμογών και δεδομένων. Το σχέδιο έχει σχεδιαστεί με στόχο την ελαχιστοποίηση του χρόνου διακοπής λειτουργίας σε περίπτωση ενός συμβάντος, τον μετριασμό των κινδύνων και τη διασφάλιση της επιχειρησιακής συνέχειας σε περίπτωση καταστροφής, είτε πρόκειται για περιστατικό κυβερνοασφάλειας, φυσική καταστροφή, βλάβη σε υλισμικό ή ανθρώπινο λάθος.

Το παρόν σχέδιο είναι ένα ζωντανό έγγραφο που υπόκειται σε τακτικές επικαιροποιήσεις για να διασφαλίζεται η καταλληλόλητα ως απάντηση στις νέες τεχνολογίες, τις αναδυόμενες απειλές και τις αλλαγές στις επιχειρηματικές διαδικασίες. Το παρόν Σχέδιο συμπληρώνει τον Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan) του οργανισμού.

## Στόχοι του Σχεδίου

Οι στόχοι του Σχεδίου με την εφαρμογή αυτού είναι οι ακόλουθοι:

* H ελαχιστοποίηση του χρόνου διακοπής λειτουργίας των κρίσιμων υπηρεσιών Πληροφορικής και Τηλεπικοινωνιών.
* Η διασφάλιση ότι η ακεραιότητα και η ασφάλεια των ευαίσθητων και κρίσιμων για τον Οργανισμό δεδομένων προστατεύονται επαρκώς από απώλεια, αλλοίωση ή μη εξουσιοδοτημένη πρόσβαση καθ' όλη τη διάρκεια της διαδικασίας ανάκαμψης.
* Ο καθορισμός σαφώς καθορισμένων στόχων χρόνου Ανάκαμψης (RTOs) και στόχων σημείου Ανάκαμψης (RPOs) για να διασφαλιστεί η ταχεία αποκατάσταση των βασικών συστημάτων και ότι αυτά μπορούν να αποκατασταθούν εντός αποδεκτών χρονικών πλαισίων.
* Ο καθορισμός ενός πλαισίου επικοινωνίας για τα εσωτερικά και εξωτερικά ενδιαφερόμενα μέρη.
* Η μείωση της οικονομικής ζημίας και της τυχόν ζημίας στην φήμη που προκαλούν οι παρατεταμένες διακοπές υπηρεσιών.
* Ο καθορισμός ρόλων και ευθυνών, αποστολών και δραστηριοτήτων για την ομάδα ανάκαμψης καταστροφών. Οι εργαζόμενοι, τα ενδιαφερόμενα μέρη και οι τρίτα μέρη είναι καλά προετοιμασμένοι για να ανταποκριθούν αποτελεσματικά σε καταστροφές και να ελαχιστοποιήσουν τις λειτουργικές διαταραχές.
* Ευθυγράμμιση του Οργανισμού με σχετικούς ρυθμιστικούς νόμους περί προστασίας δεδομένων και κυβερνοασφάλειας όπως η Απόφαση Κ.Δ.Π 389/2020, διασφαλίζοντας την τήρηση των νομικών υποχρεώσεων.
* Οι τακτικές δοκιμές μέσω ασκήσεων των διαδικασιών ανάκαμψης από καταστροφές μέσω επιτραπέζιων ασκήσεων (tabletop), προσομοιώσεων και δοκιμών πλήρους αποκατάστασης.
* Η ενσωμάτωση των διδαγμάτων που εξάχθηκαν μετά από πραγματικά περιστατικά και ασκήσεις με στόχο τη συνεχή βελτίωση στις στρατηγικές ανάκαμψης.
* Η παροχή προγραμμάτων κατάρτισης στους εργαζομένους, εξασφαλίζοντας την ευαισθητοποίηση σχετικά με την ενεργοποίηση και την εκτέλεση του Σχεδίου.

## Πεδίο εφαρμογής του σχεδίου

Το πεδίο εφαρμογής του Σχεδίου Ανάκαμψης από καταστροφές καλύπτει όλα τα συστήματα, τις εφαρμογές και τις υποδομές ΤΠ που υποστηρίζουν τις λειτουργίες του [Όνομα Οργανισμού] όπως έχουν οριστεί από την ανάλυση Εκτίμησης Επιχειρηματικών Επιπτώσεων (BIA), διασφαλίζοντας ότι οι κρίσιμες υπηρεσίες μπορούν να αποκατασταθούν εντός των καθορισμένων χρονικών στόχων Ανάκαμψης (RTO) και των στόχων ανάκτησης (RPO).

Συγκεκριμένα, το παρόν σχέδιο καλύπτει:

* **Υποδομές ΤΠ**: Κέντρα δεδομένων, στοιχεία δικτύου και τηλεπικοινωνιών, περιβάλλοντα cloud, και υλισμικό στις εγκαταστάσεις του [Όνομα Οργανισμού].
* **Εφαρμογές και βάσεις δεδομένων**: Κρίσιμα λογισμικά και άλλα συστήματα, βάσεις δεδομένων και άλλες υποστηρικτικές εφαρμογές.
* **Συστήματα διαχείρισης δεδομένων και δημιουργίας αντιγράφων ασφαλείας:** Στρατηγικές για αντιγραφή δεδομένων, αποθήκευση εκτός κτηρίου του [Όνομα Οργανισμού] και λύσεις ανάκτησης με βάση το cloud.
* **Μέτρα κυβερνοασφάλειας και συμμόρφωσης:** Εξασφάλιση ασφαλούς ανάκαμψης για την αποτροπή εκμετάλλευσης ευπαθειών κατά τη διάρκεια σεναρίων καταστροφής.
* **Επικοινωνία & αντιμετώπιση περιστατικών:** Κατευθυντήριες γραμμές για την ενημέρωση των εργαζομένων, της διοίκησης, των ρυθμιστικών αρχών και των τρίτων προμηθευτών/συνεργατών κατά τη διάρκεια ενός συμβάντος.
* **Εξαρτήσεις από εξωτερικούς προμηθευτές/συνεργάτες:** Συντονισμός με εξωτερικούς παρόχους υπηρεσιών και παρόχους διαχειριζόμενων υπηρεσιών πληροφορικής και τηλεπικοινωνιών.

## Ορισμοί

Για τους σκοπούς του παρόντος εγγράφου χρησιμοποιούνται οι ακόλουθοι ορισμοί. Οι ορισμοί αυτοί ορίζονται ευρέως σε διάφορα πρότυπα ασφάλειας πληροφοριών όπως ISO27001 και NIST και έχουν υιοθετηθεί και στην Απόφαση Κ.Δ.Π 389/2020:

* **Στοιχείο ενεργητικού:** Ένα στοιχείο που προσφέρει αξία στον οργανισμό. Ο όρος "ενεργητικό" δεν περιορίζεται μόνο σε στοιχεία υλισμικού, αλλά επεκτείνεται και σε άλλα στοιχεία όπως λογισμικό, δεδομένα, ανθρώπινο δυναμικό και φήμη.
* **Απειλή:** Μια πιθανή αιτία ενός συμβάντος, που μπορεί να οδηγήσει σε βλάβη των συστημάτων και του οργανισμού.
* **Ευπάθεια:** Μια αδυναμία ή σφάλμα σε ένα πληροφοριακό σύστημα που μπορεί να εκμεταλλευτεί από μια απειλή, θέτοντας σε κίνδυνο την ασφάλεια του συστήματος.
* **Κίνδυνος:** Αναφέρεται στις συνέπειες που μπορεί να προκύψουν για έναν οργανισμό και τα ενδιαφερόμενα μέρη του, λόγω των απειλών και των ευπαθειών που σχετίζονται με τη λειτουργία και τη χρήση των συστημάτων πληροφοριών, καθώς και με το περιβάλλον στο οποίο αυτά τα συστήματα δραστηριοποιούνται.
* **Εμπιστευτικότητα:** Η διασφάλιση ότι οι πληροφορίες δεν είναι προσβάσιμες σε μη εξουσιοδοτημένους χρήστες, διαδικασίες ή άλλες.
* **Ακεραιότητα:** Η ακεραιότητα διασφαλίζει τη συνέπεια, την ακρίβεια και την αξιοπιστία των δεδομένων..
* **Διαθεσιμότητα:** Η διαθεσιμότητα διασφαλίζει ότι οι πληροφορίες ή οι υπηρεσίες είναι προσβάσιμες όταν μια εξουσιοδοτημένη οντότητα απαιτεί πρόσβαση.
* **Έλεγχος:** Προστασία ή αντίμετρα για την αποφυγή, τον εντοπισμό, την εξουδετέρωση ή την ελαχιστοποίηση των κινδύνων ασφαλείας για τη φυσική ιδιοκτησία, τις πληροφορίες, τα συστήματα υπολογιστών ή άλλα περιουσιακά στοιχεία.
* **Σχέδιο επιχειρησιακής συνέχειας (BCP):** Τεκμηριωμένες διαδικασίες που καθοδηγούν τους οργανισμούς να ανταποκριθούν, να ανακτήσουν, και να επαναφέρουν σε προκαθορισμένο επίπεδο λειτουργίας μετά από διακοπή.
* **Ανάλυση επιχειρηματικών επιπτώσεων (BIA):** Η διαδικασία ανάλυσης των λειτουργικών λειτουργιών και εντοπισμού των επιπτώσεων που μπορεί να έχει μια διαταραχή σε αυτές.
* **Σχέδιο Ανάκαμψης καταστροφών (DRP):** Καθορισμένες και τεκμηριωμένες διαδικασίες ανάκτησης των υποδομών ΤΠ μετά από μια διαταραχή.
* **Διακοπή:** συμβάν, είτε αναμενόμενο (π.χ. τυφώνας) είτε απρόβλεπτο (π.χ. διακοπή ρεύματος, σεισμός ή επίθεση σε συστήματα/υποδομές ICT) που διαταράσσει την κανονική πορεία λειτουργίας σε χώρο του οργανισμού.
* **Στόχος χρόνου Ανάκαμψης (RTO):** Χρονική περίοδος εντός της οποίας πρέπει να ανακτηθούν τα ελάχιστα επίπεδα υπηρεσιών ή/και προϊόντων και τα υποστηρικτικά συστήματα, εφαρμογές ή λειτουργίες μετά από διακοπή.
* **Στόχος σημείου ανάκτησης (RPO):** Χρονική στιγμή κατά την οποία τα δεδομένα πρέπει να ανακτηθούν μετά από διακοπή.

## Παραδοχές

Για την ορθή εφαρμογή του Σχεδίου, γίνονται οι εξής παραδοχές:

* Όλα τα κρίσιμα δεδομένα αντιγράφονται και αποθηκεύονται και τηρούνται αντίγραφα ασφαλείας.
* Οι εργαζόμενοι εκπαιδεύονται σε τακτική βάση στις διαδικασίες Ανάκαμψης μετά από καταστροφή.
* Διατίθεται εναλλακτικός χώρο ο οποίος μπορεί να ενεργοποιηθεί όταν είναι απαραίτητο και να συνεχίσει τις βασικές λειτουργίες σύμφωνα με τις απαιτήσεις RTO των φιλοξενούμενων εφαρμογών.

## Προβλεπόμενο κοινό του Σχεδίου

Το Σχέδιο Ανάκαμψης από Καταστροφές (DRP) απευθύνεται σε βασικούς ενδιαφερόμενους του [Όνομα Οργανισμού], εργαζομένους και εξωτερικούς συνεργάτες που εμπλέκονται στο σχεδιασμό, την εκτέλεση και την εποπτεία των εργασιών ανάκαμψης από καταστροφές και επιχειρησιακής συνέχειας βάσει του παρόντος σχεδίου.

Συνιστάται η διανομή του παρόντος εγγράφου σε όλους τους ενδιαφερόμενους φορείς για την πρώτη και τις επακόλουθες κύριες εκδόσεις του εγγράφου. Πιθανοί παραλήπτες δύναται να είναι μεταξύ άλλων:

1. Μέλη της ηγεσία και της ανώτατης διοίκησης
2. Μέλη της ομάδας ανάκαμψης από καταστροφές
3. Προσωπικό του Τμήματος Πληροφορικής και της Ασφάλειας Πληροφοριών
4. Εκπρόσωποι επιχειρησιακών μονάδων
5. Πάροχοι υπηρεσιών και άλλα τρίτα μέρη

## Φύλαξη Εγγράφου

Λόγω της κρισιμότητας και της σημαντικότητας του Σχεδίου, αυτό θα πρέπει να αποθηκεύεται με ασφάλεια, να είναι εύκολα προσβάσιμο στα άτομα που εμπλέκονται και να ενημερώνεται τακτικά για να διασφαλίζεται η αποτελεσματικότητα του. Στο πίνακα πιο κάτω παρουσιάζεται η αποθήκευση της τελευταίας έκδοσης της Σχεδίου.

|  |  |  |
| --- | --- | --- |
| Κύρια αποθήκευση | Ηλεκτρονική μορφή (Electronic copy):  [ηλεκτρονική διεύθυνση που είναι φυλαγμένο το έγγραφο π.χ. intranet] | Αντίγραφο σε χαρτί (Paper Copy):  [Αντίγραφο 1 : Box file στο γραφείο του Προιστάμενου του Τμήματος Πληροφορικής  Αντίγραφο 2 : Box file στο DR Site |
| Εφεδρική αποθήκευση Σχεδίου |  |  |

## Ρόλοι και ευθύνες του Σχεδίου Ανάκαμψης Καταστροφών

Η Ομάδα Ανάκαμψης από Καταστροφές είναι υπεύθυνη για την εκτέλεση, τη διαχείριση και το συντονισμό όλων των δραστηριοτήτων που περιγράφονται στο παρόν Σχέδιο Ανάκαμψης από Καταστροφές, προκειμένου να διασφαλιστεί η έγκαιρη αποκατάσταση των κρίσιμων υπηρεσιών, λειτουργιών και συστημάτων. Η Ομάδα απαρτίζεται από τους πιο κάτω:

| **Ρόλος** | **Βασικές Αρμοδιότητες** |
| --- | --- |
| Επικεφαλής ομάδας σχεδίου Ανάκαμψης καταστροφών.\* | * Επιβλέπει την εκτέλεση του Σχεδίου (DRP), * Συντονίζει τις προσπάθειες ανάκαμψης * Λήψη αποφάσεων |
| Επικεφαλής Τμήματος Πληροφορικής και η Ομάδα Πληροφορικής | * Συντονίζει τις ενέργειες για αποκατάσταση εξυπηρετητών, δικτύων και άλλου σχετικού εξοπλισμού. * Διασφαλίζει την ανάκτηση και τη λειτουργικότητα των επιχειρησιακών εφαρμογών. * Επαναφέρει βάσεις δεδομένων και διασφαλίζει την ακεραιότητα των δεδομένων |
| Υπεύθυνος επικοινωνίας | * Ειδοποιεί τα ενδιαφερόμενα μέρη, τους εργαζομένους και τις εξωτερικές οντότητες/συνεργάτες. |

Πίνακας 1: Ιδιότητα μέλους ομάδας DRP. Να τροποποιηθεί ανάλογα με τις καθορισμένες ομάδες του Οργανισμού

\*Μπορεί να είναι και ο Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ)

## Επικεφαλής ομάδας σχεδίου Ανάκαμψης καταστροφών

Ο επικεφαλής της ομάδας ανάκαμψης είναι ο ηγέτης της ομάδας του Σχεδίου Ανάκαμψης Καταστροφών (DRP). Ο πρωταρχικός ρόλος του ατόμου είναι να καθοδηγήσει τη διαδικασία ανάκαμψης από καταστροφές και να συντονίσει όλη την υπόλοιπη ομάδα του Σχεδίου. Συστήνεται όπως καθοριστεί ένα άτομο ως αναπληρωτής, σε περίπτωση που ο επικεφαλής δεν είναι διαθέσιμος.

Πρωταρχικές αρμοδιότητες του επικεφαλής του Σχεδίου Ανάκαμψης Καταστροφών είναι:

* Χρονικός καθορισμός ενεργοποίησης του Σχεδίου με βάση τη σοβαρότητα του περιστατικού και τον αντίκτυπο στην επιχείρηση.
* Λήψη σχετικών αποφάσεων κατά τη διάρκεια ενός περιστατικού, όταν ενεργοποιείται το σχέδιο.
* Ενημέρωση της ομάδας DRP ότι το σχέδιο είναι ενεργοποιημένο και ο συντονισμός των δραστηριοτήτων του.
* το σημείο επαφής για όλη την επικοινωνία της ομάδας DRP και έρχεται σε επαφή με τον επικεφαλής της ομάδας διαχείρισης επιχειρησιακής συνέχειας (BCP), όπου εφαρμόζεται, συντονίζοντας τις αποφάσεις που πρέπει να ληφθούν.
* Ηγείται των ανασκοπήσεων μετά από μια καταστροφή για την αξιολόγηση των διδαγμάτων που αντλήθηκαν και την ανάλογη επικαιροποίηση του Σχεδίου.
* Βεβαίωση ότι το σχέδιο ενημερώνεται σε τακτική βάση.

## Επικεφαλής Τμήματος Πληροφορικής και η Ομάδα Πληροφορικής

Η ομάδα DRP αποτελείται από μέλη του προσωπικού του Τμήματος Πληροφορικής που είναι υπεύθυνα για τη διασφάλιση ότι οι λειτουργίες/ διαδικασίες/ δραστηριότητες του [Όνομα Οργανισμού] λειτουργούν σε αποδεκτό επίπεδο από εναλλακτική τοποθεσία, εντός των ισχυόντων χρονικών περιορισμών. Οι κύριες αρμοδιότητές τους είναι:

* Επιβεβαιώνει ότι ο εναλλακτικός εξοπλισμός τοποθεσίας πληροί τα καθορισμένα RTOs για όλες τις επιχειρησιακές εφαρμογές.
* Ρύθμιση όλων των συνδέσεων δικτύου, του εξοπλισμού και άλλου υλικού στην εναλλακτική τοποθεσία.
* Ρύθμιση όλων των λειτουργικών συστημάτων και εφαρμογών, επαναφορά όλων των κρίσιμων δεδομένων από αντίγραφα ασφαλείας και δημιουργία ακεραιότητας δεδομένων στην εναλλακτική τοποθεσία.
* Παροχή κατάλληλης διαχείρισης, στελέχωσης και τεχνικής υποστήριξης στους χρήστες του εναλλακτικού σημείου.
* Καθορισμός ότι πληρούνται οι ελάχιστες απαιτήσεις λειτουργίας για όλες τις κρίσιμες εφαρμογές.
* Εκτέλεση δραστηριοτήτων δημιουργίας αντιγράφων ασφαλείας στο χώρο Ανάκαμψης καταστροφών.
* Παροχή συνεχούς τεχνικής υποστήριξης στον τόπο Ανάκαμψης καταστροφών.
* Σταδιακή αποκατάσταση όλων των τοπικών και παγκόσμιων συνδέσεων δικτύου και τηλεπικοινωνιών ώστε να ανταποκρίνονται στις απαιτήσεις επεξεργασίας.
* Προμήθεια του απαιτούμενου εξοπλισμού και άλλο υποστηρικτικού υλικό το οποίο κρίνεται αναγκαίο για την εκτέλεση του Σχεδίου.
* Προσδιορισμός ότι όλα τα απαιτούμενα έγγραφα (π.χ. πρότυπα, αρχεία ζωτικής σημασίας και εγχειρίδια εφαρμογής) αποθηκεύονται σε ασφαλή θέση εκτός του χώρου.

## Υπεύθυνος επικοινωνίας

* Ο Υπεύθυνος επικοινωνίας διασφαλίζει την ορθή ενημέρωση τόσο των εσωτερικών και εξωτερικών ενδιαφερομένων για τη διαδικασία ανάκαμψης από καταστροφές. Πιο συγκεκριμένα αναλαμβάνει:
  + Την εσωτερική επικοινωνία των εργαζομένων και άλλα στελέχη της Ανώτατης Διεύθυνσης του [Όνομα Οργανισμού] για τις επιπτώσεις της καταστροφής και την πρόοδο της ανάκαμψης.
  + Την εξωτερική επικοινωνία με ρυθμιστικές αρχές και άλλα ενδιαφερόμενα μέρη.
  + Τις δημόσιες σχέσεις (PR) και διαχείριση περιστατικών ή κρίσεων κυρίως όσο αφορά τα μέσα μαζικής ενημέρωσης και τα μέσα κοινωνικής δικτύωσης (ΜΚΔ).

## Σχέδιο Ανάκαμψης καταστροφών

## Στρατηγική Ανάκαμψης καταστροφών

Σε περίπτωση συμβάντος που οδηγεί σε διακοπή της ομαλής διεκπεραίωσης κρίσιμων λειτουργιών/ διαδικασιών/ δραστηριοτήτων, ο [Όνομα Οργανισμού] θα διασφαλίσει ότι οι αυτές μπορούν να ανακτηθούν στο κατάλληλο επίπεδο και εντός του χρονικού πλαισίου που απαιτείται για την επιστροφή στις κανονικές λειτουργίες, με ελάχιστο αντίκτυπο στη λειτουργία του [Όνομα Οργανισμού].

Το Σχέδιο Ανάκαμψης Καταστροφών (DRP) αποτελεί υποσύνολο του Σχεδίου Επιχειρησιακής Συνέχειας (BCP) και περιγράφει τις διαδικασίες που πρέπει να ακολουθηθούν σε σχέση με την ανάκτηση και τη συνέχεια των λειτουργιών/ διαδικασιών/ δραστηριοτήτων που στηρίζουν τις επιχειρησιακές δραστηριότητες του [Όνομα Οργανισμού].

Το Σχέδιο προϋποθέτει την ύπαρξη εναλλακτικής τοποθεσίας (δηλαδή τόπου Ανάκαμψης καταστροφών). Σε περίπτωση που υπάρχει εναλλακτική τοποθεσία Ανάκαμψης, η διοίκηση σε συνεργασία με το Τμήμα Πληροφορικής του [Όνομα Οργανισμού] πρέπει να επιβεβαιώσουν ότι είναι διαθέσιμοι οι απαιτούμενοι πόροι και εφαρμογές για κάθε κρίσιμη επιχειρησιακή διαδικασία.

Το Κέντρο Δεδομένων Ανάκαμψης Καταστροφών υποχρεούται να παρέχει τους ελάχιστους πόρους που απαιτούνται για τη συνέχιση των υπηρεσιών (δηλαδή τη φιλοξενία εικονικών μηχανών και δεδομένων) που υποστηρίζουν τις κρίσιμες επιχειρησιακές διαδικασίες του οργανισμού, όπως ορίζονται στην Εκτίμηση Επιχειρηματικών Επιπτώσεων. Τα χρονικά πλαίσια ανάκτησης πρέπει να πληρούν τις απαιτήσεις Στόχου Χρόνου Ανάκαμψης (RTO) και Στόχου Σημείου Ανάκτησης (RPO) ανά επιχειρησιακή εφαρμογή.

Σε περίπτωση συμβάντος, η πρώτη προτεραιότητα του οργανισμού είναι να αποτρέψει την απώλεια ζωών. Πριν ληφθούν δευτερεύοντα μέτρα, ο [Όνομα Οργανισμού] θα διασφαλίσει ότι όλοι οι εργαζόμενοι, και οποιαδήποτε άλλα άτομα βρίσκονται στις εγκαταστάσεις που ελέγχονται από τον οργανισμό, είναι σώα και αβλαβή.

O επόμενος στόχος του Σχεδίου είναι οι εκτέλεση των βημάτων που περιγράφονται σε αυτό το έγγραφο για επαναφορά όλων των δραστηριοτήτων όσο το δυνατόν συντομότερα. Αυτό περιλαμβάνει:

* Αποτροπή απώλειας εσωτερικών πόρων του [Όνομα Οργανισμού], όπως υλισμικού, δεδομένων και φυσικών στοιχείων πληροφορικής.
* Ελαχιστοποίηση της απώλειας επικοινωνίας δεδομένων με εξωτερικές εξαρτήσεις.
* Ελαχιστοποίηση του χρόνου διακοπής λειτουργίας που σχετίζεται με Πληροφοριακά Συστήματα.
* Διατήρηση της λειτουργίας των επιχειρηματικών δραστηριοτήτων σε περίπτωση καταστροφής.

Σκοπός αυτής της στρατηγικής είναι να διασφαλίσει ότι ένα πληροφοριακό σύστημα και η ανάκτηση δεδομένων του οργανισμού ελέγχονται με σαφείς ευθύνες και λογοδοσία, διασφαλίζοντας ότι:

* Εντοπίζονται οι βασικές εφαρμογές, η υποδομή δικτύου και διακομιστών, οι επικοινωνίες, η αποθήκευση δεδομένων και τα συστήματα δημιουργίας αντιγράφων ασφαλείας
* Η ανάλυση επιχειρηματικών επιπτώσεων και η αξιολόγηση κινδύνου εφαρμόζονται σε αυτές τις βασικές εφαρμογές, υποδομές, επικοινωνίες και συστήματα αποθήκευσης
* Τα πληροφοριακά συστήματα και η ανάκτηση δεδομένων έχουν δοκιμαστεί και βελτιωθεί με στόχο να διασφαλιστεί η συνέχεια των βασικών δραστηριοτήτων σε ένα ελάχιστο αποδεκτό πρότυπο σε περίπτωση συμβάντος διακοπής.
* Η ανώτατη διοίκηση του [Όνομα Οργανισμού] μπορεί να είναι βέβαιη ότι όλα τα στοιχεία που σχετίζονται με το πληροφοριακό σύστημα και την ανάκτηση δεδομένων παραμένουν ενημερωμένα, σχετικά, αποτελεσματικά και υπό συνεχή βελτίωση.

Κάθε μέλος του προσωπικού πρέπει να συμμορφώνεται με αυτή τη στρατηγική και αναμένεται να συμβάλει στην ελαχιστοποίηση των κινδύνων για τις λειτουργίες του οργανισμού και να ενισχύσει τη θέση και τη φήμη του [Όνομα Οργανισμού] στους δικαιούχους και στα ενδιαφερόμενα μέρη του.

Η προσέγγιση ανάκαμψης καταστροφών είναι η υποστήριξη του οργανισμού σε περίπτωση που ο κύριος χώρος του οργανισμού δεν είναι πλέον λειτουργικός.

## Ανάλυση επιχειρηματικών επιπτώσεων (BIA) - Καθορισμός Κρίσιμων λειτουργιών

Όπως αναφέρεται και πιο πάνω, βασικός στόχος του Σχεδίου είναι η υποστήριξη της ανθεκτικότητας των κρίσιμων δεδομένων και συστημάτων που προσδιορίστηκαν κατά τη διάρκεια της **Ανάλυση επιχειρηματικών επιπτώσεων (BIA)**  και πρέπει όπου εφαρμόζεται να ευθυγραμμιστεί με τις διατάξεις του Σχεδίου Επιχειρησιακής Συνέχειας (BCP). Οι πιο σημαντικές επιχειρησιακές λειτουργίες του [Όνομα Οργανισμού] που καταγράφηκαν στην ΒΙΑ, είναι οι ακόλουθες:

- κρίσιμη λειτουργία 1

- κρίσιμη λειτουργία 2

Κτλ.

Για αυτές τις [να αναφερθεί ο αριθμός] πιο πάνω κρίσιμες επιχειρηματικές λειτουργίες του [Όνομα Οργανισμού] έχουν αναπτυχθεί συγκεκριμένα σχέδια ανάκαμψης από καταστροφές για την αντιμετώπιση της απώλειας δεδομένων ή/και μη διαθεσιμότητας του πρωτεύοντος κέντρου δεδομένων.

|  |  |  |  |
| --- | --- | --- | --- |
| Α/Α | Κρίσιμη λειτουργία | Κρίσιμα στοιχεία & άλλα υποστηρικτικά υποσυστήματα | Σχέδιο Ανάκαμψης |
| 1 | κρίσιμη λειτουργία 1 | Εξυπηρετητής 1  Βάση δεδομένων ...  Web Server… | Βλέπε παράρτημα – Στα παραρτήματα να υπάρχει Τμήμα το οποίο να καταγράφει το αναλυτικό σχέδιο Ανάκαμψης της λειτουργίας |
| 2 | κρίσιμη λειτουργία 2 |  |  |

## Πίνακας κρισιμότητας Ανάκαμψης καταστροφών (DR Criticality Matrix)

Ο παρακάτω πίνακας αναλύει τα αποτελέσματα της **Ανάλυση επιχειρηματικών επιπτώσεων (BIA)** A σύμφωνα με την αναγνωρισμένη κρισιμότητα των RTO και RPO δεδομένων και επικεντρώνεται στην εξυπηρέτηση των στόχων του Σχεδίου. Ο πίνακας (παράδειγμα) λαμβάνει υπόψη δεδομένα που έχουν βαθμολογηθεί ως πολύ κρίσιμα, υψηλό και μέτρια.

|  |  |  |  |
| --- | --- | --- | --- |
| Σύστημα/Λειτουργία | RTO (Recovery Time Objective) | RPO (Recovery Point Objective) | Αντίκτυπος του χρόνου διακοπής λειτουργίας |
| Βάσει Δεδομένων | 4 ώρες | 30 λεπτά | πολύ κρίσιμο |
| Email Services | 8 ώρες | 30 λεπτά | υψηλό |
| xx |  |  |  |
| xx |  |  |  |

## Σενάρια

Το Σχέδιο καταστροφών λαμβάνει σενάρια για αποκατάσταση όλων των ακόλουθων τεχνολογικών τομέων:

* Δικτυακή Υποδομή
* Παροχή Ενέργειας
* Υποδομή διακομιστών
* Σύστημα τηλεφωνίας
* Συστήματα αποθήκευσης και δημιουργίας αντιγράφων ασφαλείας δεδομένων
* Κρίσιμες Επιχειρηματικές Εφαρμογές
* Συνδεσιμότητα με σημαντικούς πόρους προμηθευτή (εάν είναι συνδεδεμένοι)
* Συνδεσιμότητα στο Διαδίκτυο
* Χώρος εργασίας χρήστη

Επιπρόσθετα συστήνεται όπως ο [Όνομα Οργανισμού] υλοποιήσει και συμπεριλάβει στο Σχέδιο, σενάρια σε μορφή Playbooks που αποσκοπούν στη παροχή μιας δομημένης προσέγγισης για την αντιμετώπιση περιστατικών βασισμένα στα τελευταίες Κυβερνοαπειλές (π.χ. Playbook για αντιμετώπιση απειλών τύπου Ransomware). Τα συγκεκριμένα Playbooks θα ανανεώνονται σε ετήσια τουλάχιστο βάση ώστε να παραμένουν επικαιροποιημένα.

## Τοποθεσία και Συνδεσιμότητα εναλλακτικού χώρου εργασίας

|  |  |  |
| --- | --- | --- |
| Κύριος χώρος εργασίας (**Primary Datacenter Location)** | Διεύθυνση | Σχόλια |
|  |  |  |
| Εναλλακτικός χώρος εργασίας (**DR Location)** | Διεύθυνση | Σχόλια |
|  |  |  |

## Λίστα ελέγχου δραστηριοτήτων και εργασιών Ανάκαμψης καταστροφών

Σε περίπτωση που διαπιστωθεί συμβάν μεγάλης κλίμακας στον οργανισμό, θα πρέπει να χρησιμοποιείται ο ακόλουθος κατάλογος ελέγχου:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Δραστηριότητα** | **Τοποθεσία** | **Υπεύθυνος** | **Χρόνος/ημερομηνία ολοκλήρωσης στόχου** | **Πραγματική ώρα/ημερομηνία ολοκλήρωσης** |
| Επικύρωση του τελευταίου αντιγράφου ασφαλείας αναπαραγωγής | Π.χ. Κεντρικά γραφεία |  |  |  |
| Ενημέρωση όλων των μελών της ομάδας Ανάκαμψης καταστροφών | Κεντρικά γραφεία |  |  |  |
| Επαλήθευση των λειτουργιών/διαδικασιών / δραστηριοτήτων που δεν είναι διαθέσιμες | Κεντρικά γραφεία |  |  |  |
| Απενεργοποίηση λειτουργιών/ διαδικασιών/ δραστηριοτήτων από τα Κεντρικά Γραφεία (κατά περίπτωση) | Κεντρικά γραφεία |  |  |  |
| Ενεργοποίηση λειτουργιών/ διαδικασιών/ δραστηριοτήτων από την τοποθεσία Disaster Recovery | Τοποθεσία DR |  |  |  |
| Αναδρομολόγηση όλης της συνδεσιμότητας με την τοποθεσία Disaster Recovery | Τοποθεσία DR |  |  |  |
| Επαλήθευση λειτουργίας λειτουργιών/ διαδικασιών/ δραστηριοτήτων εντός της τοποθεσίας Disaster Recovery | Τοποθεσία DR |  |  |  |
| Επαλήθευση συνδεσιμότητας και λειτουργίας λειτουργιών/ διαδικασιών/ δραστηριοτήτων από τα Κεντρικά Γραφεία | Κεντρικά γραφεία |  |  |  |
| Απενεργοποίηση λειτουργιών/ διαδικασιών/ δραστηριοτήτων από την τοποθεσία Disaster Recovery | Τοποθεσία DR |  |  |  |
| Ενεργοποίηση λειτουργιών/ διαδικασιών/ δραστηριοτήτων από τον Κύριο Ιστότοπο | Κεντρικά γραφεία |  |  |  |
| Αναδρομολόγηση όλης της συνδεσιμότητας με τα Κεντρικά Γραφεία | Κεντρικά γραφεία |  |  |  |
| Επαλήθευση λειτουργίας λειτουργιών/ διαδικασιών/ δραστηριοτήτων εντός των Κεντρικών Γραφείων | Κεντρικά γραφεία |  |  |  |
| Επαλήθευση συνδεσιμότητας και λειτουργίας λειτουργιών/ διαδικασιών/ δραστηριοτήτων από τα Κεντρικά Γραφεία | Κεντρικά γραφεία |  |  |  |

Πίνακας 2: Κατάλογος ελέγχου Ανάκαμψης καταστροφών

## Συντήρηση και δοκιμές του Σχεδίου

## Αναθεώρηση σχεδίων και χρονοδιάγραμμα

Το σχέδιο Ανάκαμψης καταστροφών θα επανεξετάζεται σε τακτική βάση (τουλάχιστον ετησίως) από τον επικεφαλής της ομάδας του σχεδίου Ανάκαμψης καταστροφών. Η επανεξέταση θα καλύπτει τουλάχιστον τα ακόλουθα στοιχεία και θα διασφαλίζει ότι εντοπίζονται και αντιμετωπίζονται τυχόν αλλαγές:

* Το εφαρμοστέο πεδίο εφαρμογής του σχεδίου (δηλαδή η αλλαγή εγκατάστασης).
* Τους ισχύοντες κινδύνους.
* Αλλαγές στις επιχειρησιακές απαιτήσεις (π.χ. η κρισιμότητα κάθε λειτουργίας/ διαδικασίας/ δραστηριότητας).
* Αλλαγή υποδομής.
* Αλλαγές στο προσωπικό, τους ρόλους και τις ευθύνες και τα στοιχεία επικοινωνίας των μελών της ομάδας.
* Αλλαγές στους προμηθευτές, στοιχεία επικοινωνίας προμηθευτών και υπηρεσιών έκτακτης ανάγκης.
* Διδάγματα από την πιθανή ενεργοποίηση του σχεδίου ή τις δοκιμές που πραγματοποιήθηκαν.
* Εξωτερικοί ή εσωτερικοί έλεγχοι.
* Εισαγωγή νέων συστημάτων.
* Ανανέωση Playbooks

## Αλλαγή διαδικασίας διαχείρισης

Οι τυχόν επικαιροποιήσεις του παρόντος σχεδίου ακολουθούν τη συνήθη διαδικασία διαχείρισης αλλαγών του [Όνομα Οργανισμού].

## Δοκιμές Ανάκαμψης καταστροφών

Οι δοκιμές του DRP έχουν σχεδιαστεί για να καθορίζουν:

* Την κατάσταση ετοιμότητας του οργανισμού να ανταποκριθεί και να αντιμετωπίσει μια διαταραχή.
* Κατά πόσον το συνολικό σχέδιο είναι επαρκές για την υποστήριξη της επανάληψης των επιχειρηματικών δραστηριοτήτων.
* Κατά πόσον τα ειδικά καθήκοντα και διαδικασίες είναι επαρκή για την υποστήριξη της επανάληψης των επιχειρηματικών δραστηριοτήτων.
* Κατά πόσον το σχέδιο έχει διατηρηθεί σωστά ώστε να αντικατοπτρίζει τις πραγματικές ανάγκες ανάκαμψης υπό το πρίσμα των επιχειρηματικών αλλαγών.

Οι παραλλαγές των δοκιμών μπορεί να περιλαμβάνουν δομημένες αναλυτικές παρουσιάσεις, προσομοιώσεις συγκεκριμένων σεναρίων ή πιο περίπλοκες δοκιμές στις περιπτώσεις διακοπής μιας υπηρεσίας. Θα πρέπει να χρησιμοποιείται μείγμα μεθόδων για να εξασφαλίζεται η αυστηρή διεξαγωγή των δοκιμών.

Τα αποτελέσματα των δοκιμών πρέπει να καταγράφονται και να διατηρούνται για τουλάχιστον τρεις κύκλους δοκιμών.

Τα αποτελέσματα των δοκιμών πρέπει να:

* Τεκμηριώνονται από την ομάδα που εκτελεί τη δοκιμή.
* Επανεξετάζονται για τυχόν κενά ή/και τομείς βελτίωσης, και να είναι συμπληρωμένα με σχέδιο δράσης για την αντιμετώπιση τυχόν κενών που εντοπίζονται.
* Επανεξετάζονται και υπογράφονται από τον επικεφαλής της ομάδας διαχείρισης καταστροφών και να τίθενται υπόψη της ανώτατης διοίκησης.

# Παράρτημα Α – Στοιχεία επικοινωνίας της ομάδας Ομάδα Ανάκαμψης από Καταστροφές

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Όνομα** | **Τίτλος** | **Τμήμα** | **Ρόλος στα σχέδια** | **Αριθμός κινητού τηλεφώνου** | **Διεύθυνση ηλεκτρονικού ταχυδρομείου** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Παράρτημα Β – Λίστες επαφών

## Εσωτερική λίστα επαφών

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Όνομα** | **Τίτλος** | **Τμήμα** | **Αριθμός κινητού τηλεφώνου** | **Αριθμός οικίας** | **Διεύθυνση ηλεκτρονικού ταχυδρομείου** |
|  |  |  |  |  |  |

## Λίστα εξωτερικών επαφών

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Κατηγορία** | **Όνομα** | **Σύντομη περιγραφή / Σκοπός** | **Τηλέφωνο** | **Διεύθυνση ηλεκτρονικού ταχυδρομείου (κατά περίπτωση)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Άλλα Παραρτήματα κατά περίπτωση – Αναλυτική περιγραφή Σεναρίων και Playbooks όπως καταγράφεται στη παράγραφο 7.4 του παρόντος σχεδίου