**UnderDefense policy template kit**

Starting your compliance journey? UnderDefense policy template offers a comprehensive and compliance-ready document, complete with placeholders for company-specific details.

**How to use this document**

1. Thoroughly review the content of each policy, analyzing it section by section.
2. Evaluate whether the subsequent section and its associated risks are applicable to you. If it does not, remove it and/or replace it with your organization’s corresponding practices.
3. Replace any highlighted text in angled brackets < >[[1]](#footnote-0) with appropriate information (Use Find to make sure that all text in angled brackets is replaced)
4. Remove this instructions page
5. Add any company-specific letterhead, branding, and formatting
6. Save this document as PDF and upload to UnderDefenseMAXI to <https://app.underdefense.com/compliance/ISO27001/approved-policies>

# The Path to Compliance

# We'll guide you through, ensuring a smooth path to compliance:



**SOC 2 Certification Timeline for SMBs with 50-250 Employees**

# 

# Need Expert Assistance?

| Navigating the complexities of compliance can be challenging, especially for businesses with limited internal resources or expertise.   * Experience team at the right time * Preparation of all compliance docs * Expert guidance on all tech-related issues   [**Book a call with expert**](https://meetings.hubspot.com/underdefense/help-with-compliance) | **Take your compliance from probable to guaranteed.** |
| --- | --- |

**<Your Company Logo>**

**Business Continuity & Disaster Recovery Plan**

# 

# Version Control Table

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 | <Date> | <Author> | Issued |
| 1.0 | <Date> | <Author> | Updated |
| 1.0 | <Date> | <Author> | Approved |
| **1.0** | <Date> | <Author> | **Granted “FINAL” status** |

| **Date of Next Revision** | **<date>** |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status and at yearly intervals after that.

The version control table will show the published update date and provide a thumbnail of the significant change. CAUTION: the thumbnail is not intended to summarize the difference and is not a substitute for reading the full text.

# ***Table of Contents***

[**The Path to Compliance 2**](#_htrkie77tuhx)

[**We'll guide you through, ensuring a smooth path to compliance: 2**](#_bor2nqthjwhg)

[**Need Expert Assistance? 2**](#_j1ad4z2lk78s)

[**Version Control Table 4**](#_7oqfmz9ribbc)

[**Table of Contents 5**](#_xxo923m8zwcm)

[**Purpose 7**](#_90ypckr0tju7)

[**Scope 7**](#_r3guvb2gp0sa)

[**Roles and responsibilities 7**](#_xx5lfa3no2l8)

[**Policy 9**](#_5cuoijzfj1zg)

[The strategy of <Company> business continuity plan 9](#_uy39454801ft)

[Plan Objectives 10](#_th32jpd2ekr6)

[The BCP will include a reference to: 10](#_aigko58hvpkg)

[Identification and management of risks and Business Impact Analysis (BIA) 10](#_emq6zs23t1om)

[Risk Mitigation Measures 10](#_wc0seukfi2xo)

[Business Continuity and Disaster Recovery Needs 12](#_j73xdrtviu93)

[Our BCP objectives: 12](#_low5prdg1be3)

[General Business Continuity Prerequisites 13](#_1il9nje6dckm)

[Disaster Recovery Activities 13](#_tqbfrd67jwp1)

[**Disasters Scenarios & Risks 13**](#_mw10rh2b3ugi)

[Natural disaster (major fire, major flood, earthquake - regardless of source) 13](#_cjjzftxrzz4v)

[Epidemic Health Situations 14](#_7x4iqcmve7sx)

[IT Incident (Data breach, Penetration, Ransomware, virus, equipment failure, communication, theft, robbery of work equipment) 15](#_jrob6cx05frl)

[IT Incident (Network outage, Power outage) 16](#_21ur5uebp3t8)

[Unavailability of Primary Internet Provider 16](#_hd3fiucz768c)

[Unavailability of Both Network Providers 16](#_3n3hmp8rjw10)

[Unavailability of Central Power Supply 16](#_xij74zsehbz1)

[Terrorism attack or Increased military aggression 17](#_dayac4mqaoon)

[Technical preparedness 17](#_cr849vr1geet)

[Organizational preparedness 17](#_nm9exteknw6l)

[Crisis communication plan and responsibilities for scenario «Man-made disaster, including radiation leakage / accident at a nuclear power plant» 18](#_gjdgxs)

[**Testing of the Business Continuity Plan 20**](#_eog2koimh8ji)

[Communication Channels 20](#_6ry9fs1thby2)

[**Disciplinary actions 20**](#_oo4pebgvtuk2)

[**Change, Review, and Update 21**](#_6cu0cv3y3y7n)

[**Responsibility 21**](#_fxvzxllev4xj)

[**Reference 21**](#_abyh665p4kb0)

[**Related Documents 21**](#_s97ivf2jlxea)

# 

# 

# 

# 

# 

# 

# 

# 

# Purpose

This document provides a framework to counteract interruptions to critical business activities and protect essential processes of business from the adverse effects of business disruptions.

# Scope

The scope of this document includes all users who have access to company-owned or company-provided computers or require access to the corporate network and systems.

This policy and plan applies to employees and guests, contractors, and anyone needing access to the corporate systems to continuously serve our customers. The scope of this plan includes business continuity, disaster recovery, escalation of war, employee safety and its potential impact on business operations.

# Roles and responsibilities

In case of a disaster, the committee is gathered to discuss the future actions needed for the system recovery. All key stakeholders are informed about the <Company> systems’ current state during the recovery from a disaster.

The Business Continuity Committee includes key members from departments across the organization. The backup personnel are defined in the table below to cope with the responsibilities of the Business Continuity Committee if, for any reason, the key member is not able to represent the BC Committee's interests.

| **Role** | **Responsibility** |
| --- | --- |
| CEO  <Name> | General Management, Business Development, Business Continuity, and Disaster Recovery, Communication with Clients |
|
| COO  <Name> | Financial Management, Physical Security, Information Security Management System, Information Security Policies Review and Approval |
|
| Head of Delivery  <Name> | Company Processes Management, <Departments Processes Management>, Development Processes Management, Communication with Clients, Information Security Management System, Information Security Policies Review and Approval |
|
| HR  <Name> | Human Resources Management, Communication with Employees and Candidates |
|
| Security Engineer  <Name> | Cloud & Internal Infrastructure |
|
| **Backup personnel** | **Responsibility** |
| Project Manager  <Name> | Physical Security, <Departments Processes Management>, Communication with Clients, Human Resources Management |
| Finance  <Name> | Financial Management, Human Resources Management |

The personnel contacts (phone number, corporate email, personal email) can be found within <Company> BCP Teams and Contacts.

<Screenshot of the personnel contacts>

The actual location, address, phone number and email can be found on the <Human resource management system> platform.

<Screenshot of Human resource management system>

<Company> Insurance Provider is <Insurance Provider Name> with POLICY NUMBER: <Number>:

APPROVED CLAIMS PANEL PROVIDERS:

* <List of providers>

Unique Market Reference No. <Number>

Layers:

* <List of Layers>

CLAIMS MANAGER:

* <Claims Manager>

<Screenshot of Insurance>

The Disaster Recovery Committee is responsible for:

* Developing and implementing strategies for recovering IT systems and data after various types of disasters or technology failures.
* Identifying critical IT assets, data repositories, and applications that need to be restored quickly.
* Planning resources and people allocation, load distribution to continue uninterrupted service delivery to our customers
* Creating and maintaining disaster recovery plans that outline procedures for recovering technology systems and data.

The Disaster Recovery Committee comprises at least the same individuals as the Disaster Recovery Committee. However, if required, specialists will be added whose expert opinions and responsibilities within the company are deemed necessary for achieving the committee's aims.

The IT Security team is composed of employees from SOC, DevOps, DevSecOps and IT who provide support for the company's current infrastructure. It includes, at least but not limited to:

1. Asset Manager
2. System Administrators
3. Network Administrator
4. Backup Administrators
5. Cloud DevOps

However, this list can be augmented if deemed necessary.

# Policy

## The strategy of <Company> business continuity plan

To develop, implement, and manage a robust and effective Business Continuity Plan (BCP) to

Protect <Company’s> operations, including its customers, employees, contractors, sub-contractors, and interested third parties.

There are three primary aspects that <Company> takes into account for its business continuity plan concerning key applications and processes:

* **High availability**: Providing the capability and processes so that a business has access to web applications regardless of local failures. These failures might be in the business processes, physical facilities, or IT hardware or software.
* **Continuous operations**: Safeguard the ability to keep things running during a disruption, as well as during planned outages such as scheduled backups, power outages, or planned maintenance.
* **Disaster recovery**: Establishing a way to recover data processing facilities at a different site if a disaster destroys the primary site.

<Screenshot with Goals, Objectives, Procedures>

### Plan Objectives

* Serves as a guide for <Company> and its recovery teams.
* Reference any relevant data that resides outside this document.
* Provide procedures and resources needed to assist in recovery.
* Identify notification procedures in the event of a disaster.
* Identify, assess, and minimize risks.
* Assist in avoiding confusion experienced during a disaster by documenting, testing, and reviewing recovery procedures.
* Document storage, safeguarding, and retrieval procedures for vital information and data.

The IT Security team has created a Business Continuity Plan in conjunction with the Disaster Recovery Committee. The Disaster Recovery Committee and Business Continuity Committee are responsible for maintaining the BCP.

The BCP will be implemented to maintain or restore critical operations within agreed timescales.

### **The BCP will include a reference to:**

* Critical <Company’s> systems
* Critical <Company’s> employees and stakeholders
* Business continuity roles and responsibilities
* Performed risk assessments
* Compliance with customers’ security requirements and contractual agreements;
* Compliance with <Company’s> information security management system (ISMS);
* Operational procedures that will ensure recovery and restoration of business operations and availability of information within agreed timescales;
* Education of relevant staff on pre-defined procedures;
* Testing and updating of plans and procedures.

### **Identification and management of risks and Business Impact Analysis (BIA)**

The IT Security team will perform annual risk assessments and Business Impact Analysis to identify issues that will affect the ability to provide services to its customers. Additional information relating to Business Continuity Planning (BCP) can be found within this document (section Scenarios section) and Business Impact Analysis results. Also, the set of important risk mitigation measures is highlighted in section Risk Mitigation Measures.

#### **Risk Mitigation Measures**

This chapter delineates the proactive measures undertaken by <Company> to identify, minimize the likelihood, and mitigate the potential impact of risks on our global business operations.

In response to the dynamic risks of today's landscape, we continuously refine our processes and bolster our business resilience.

Over the past two years, aligning with global events, we have adopted a strategy of global business diversification, resulting in the following key advantages:

* Global Team Distribution:
  + <Company> team is strategically distributed across various locations:
    - <XX>% in the US
    - <XX>% in Western Europe
    - <XX>% of employees can be relocated to the EU within 16 hours
    - <XX>% in other countries (Canada, Germany, Spain, etc.)
    - Each team has representatives in different countries to minimize location-specific risks.
* Cloud-Based Infrastructure:
  + The entire infrastructure, including Infrastructure as a Service (IaaS) and Software as a Service (SaaS), is cloud-based, enhancing flexibility and resilience. No client data is stored or processed in internal DC. Customer data is processed or stored only in tenant in geo location of country to compliance with. E.g. Canadian customers have AWS instances in Canada.
* Site-to-Site Virtual Private Networks (S2S VPN):
  + Secure and available S2S VPNs are established to facilitate remote work. 2FA is enabled on all client-side connections. PKI is in use for S2S with customers who enabled these connections. Keys rotation is performed every 1Y.
* Secure Offices:
  + We have biggest human hubs with offices in
    - <City, Country, description>
    - <City, Country, description>
    - <City, Country, description>
  + We have followed-the-sun 24x7 team on duty distributed globally. The absence of service capability at one location is immediately compensated by seamless delivery from other locations, enabling uninterrupted service to our clients. We test and balance load every 6 months.
* Alternative Business Operation Locations:
  + We have created and maintained alternative locations in the EU, USA, etc. to ensure continuity of business operations.
* Uninterrupted Power and Energy Sources:
  + In the locations with some risk factor we equipped the uninterrupted power sources, alternative energy supplies and fuel generators for electricity.
* Redundant Communication Channels:
  + Each location is furnished with alternative communication sources (2 internet providers). In the locations with some risk factor we equipped 3rd satellite internet channel based on Starlink.
* Regular Training and Testing:
  + <Company> conducts regular training sessions (every 6 months) and tests for emergency situations and tools to minimize potential consequences.
* Crisis Committee for each Risk factor:
  + A dedicated Crisis Committee is organized for each identified risk, equipped with detailed action plans for various scenarios.
* Communication of BC/DR Plan:
  + The Business Continuity/Disaster Recovery (BC/DR) plan has been communicated to all employees, ensuring preparedness for emergency situations.

By implementing these comprehensive risk mitigation measures, <Company> fortifies its global operations against potential disruptions, exemplifying a proactive approach.

Through effective implementation of measures, <Company> has not yet experienced any business interruption incidents since company establishment.

## Business Continuity and Disaster Recovery Needs

Our Business Continuity Strategies includes:

Pre-Escalation:

* Employee communication and training
* Remote work policies and infrastructure
* Data backup and cybersecurity measures
* Insurance coverage review
* Supply chain contingency plans

In Case of Escalation:

* Evacuation procedures and safe havens
* Shelter-in-place protocols and emergency supplies
* Communication protocols and reporting mechanisms
* Financial and mental health support for employees

Post-Escalation:

* Damage assessment and recovery strategies
* Employee wellbeing and support programs
* Business resumption planning (remote work, relocation, office repairs)

## Our BCP objectives:

* There should be the capability to ensure Business Continuity for 72 hours following any Critical Situation.
* The technical environment should be recovered within the specified timelines (up to 8h).
* The business process should be fully recovered within specified timelines (up to 4h).

## General Business Continuity Prerequisites

1. Internet access should be provided by several separate ISPs (at least two), with a main and a backup Internet connection. Failover and load balancing, with automated switching should be available. IP addresses should be whitelisted on customer side.
2. Encrypted Data backups should be stored on-site (<e.g. AWS>) and off-site.
3. Key employees should have corporate laptops configured adequately with a sufficient level of security.
4. All employees should be able to work outside of the company office in case of a Critical Situation.

## Disaster Recovery Activities

1. <Company> employees and clients should be notified as soon as possible via email and phone call.
2. <Company> employees and clients should be provided with periodic updates during the Critical Situation and its Recovery (performed via <Service Name>).
3. Notification should be done via an email message, following a phone call to appropriate stakeholders.
4. The Recovery efforts should be coordinated with the key stakeholders.
5. The most recent verified backup should be used to restore data and files.
6. The document Recovery efforts should be appropriate to the value of the losses.
7. The integrity of restoring systems and data should be verified before re-releasing into production.
8. All the other necessary Recovery activities should be taken according to the circumstances.

# Disasters Scenarios & Risks

We have developed and implemented a Business Continuity Plan (BCP) for <Company> where the most risky scenarios were taken into consideration in order to keep up and running our critical business processes, functions and activities.

### **Natural disaster (major fire, major flood, earthquake - regardless of source)**

Upon discovery of a disaster, the following procedures should be followed:

1. Local HR or teams that are located in impacted geographic areas should immediately inform all employees and contractors of the danger.
2. Order everyone to leave the danger zone, Head of HR should and PM team coordinate employees relocation to the safe location.
3. Local managers/employees should immediately report to local emergency services about the situation.
4. Employees/Contractors should leave the danger zone as soon as possible.
5. Employees/Contractors must assist other team mates, customers and guests during the evacuation.
6. If you are not near the workplace - it is forbidden to return to it and try to take away any material resources, everyone must immediately go to the safety zone.
7. If an employee or contractor is in the workplace near valuable resources, such as money, important documents, laptops, and others in his area of ​​responsibility, he can take them out of the area of ​​danger only if it does not require additional time, does not interfere with evacuation and does not endanger people.
8. Project and team leaders need to make sure during the evacuation process that none of their teams remain in danger.
9. Provide the arriving rescue services with the necessary information about possible victims and people they cannot find.
10. Provide primary care to victims while in the safety zone.
11. Once people are safe, start implementing disaster recovery and business continuity plans.
12. Head of HR should take care of employees affected and their families from the “Emergency budget”.
13. Inform customers if the situation has affected them or could potentially affect them in the future, and indicate the approximate time of resumption of services.

### **Epidemic Health Situations**

<Company> will advise each contributor/employee/contractor to work from their homes to minimize the risk in case of epidemic health developments.

The additional measures to mitigate the issue are the following ones:

1. Follow the instructions of the World Health Organization (WHO) and other government institutions.
2. Disinfects are installed along with a thermometer to check each person that enters <Company’s> office.
3. Remote shifts are enforced. Full remote is initiated in case more than 6 people are impacted.
4. Office presence is analyzed to track infection chains.
5. Monitor the situation and government enforcement regarding the matter.
6. Head of HR is in charge of monitoring employees' health issues, and helping them to recover quickly, guiding and consulting them and their relatives.

It is expected that in such a distributed environment - no more than 30% of staff should be impacted. Timing is everything.

Each employee/contractor with symptoms must inform their teammates, PM and Head of HR about the disease.

In case of a contagious infection, a quarantine is required, and the employee should be provided with all necessities to work remotely from home.

<Company> strongly recommends their employees get vaccinated from COVID 2019.

### **IT Incident (Data breach, Penetration, Ransomware, virus, equipment failure, communication, theft, robbery of work equipment)**

In the event of loss of control over the workstation hardware because of, but not limited to, theft or virus infection, the following actions should be taken to ensure the safest path to resolve this incident.

1. IT Incident Response Team and employee Manager - must be informed immediately via email or direct call to <Company> Emergency Support <Number>.
2. The Incident Response Team investigates the situation and assigns a severity to the threat, <Defined SOC analyst> and IR team would start investigation immediately.
3. Any credentials to the systems which could be stored on the workstation or mobile device must be revoked.
4. In the case of a virus infection, any infected device must be shut down as soon as possible. Employees who were impacted - should take additional training on KnowBe4 platform. Manager should be notified. SOC validates if this is part of targeted campaign or accidental
5. Impact assessment should be done by <Company> CISO.
6. Until the Incident Response Team clears a device following a reported incident, its use is prohibited.
7. Analysis of the causes and consequences of the incident, implementation of changes, training of employees

Detailed information on the management of security incidents involving <Company> and its clients' information and information technology resources can be found in the <Company> Incident Response Plan.

Activate our Professional Liability & Cyber Insurance by <Cyber Insurance>

Cyber incident helpline:

<Number>

### **IT Incident (Network outage, Power outage)**

#### ***Unavailability of Primary Internet Provider***

In this scenario, if the primary internet provider becomes unavailable, an automatic switch to the secondary network provider is configured (failover). No delays are expected, and there is no need for additional communication regarding this incident with the Asset Manager.

#### ***Unavailability of Both Network Providers***

If both network providers are unable to provide their services, any employee/contractor who discovers this issue must notify the Asset Manager immediately. If the Asset Manager is unavailable, the Chief Operating Officer (COO) should be notified. This notification should be made through any accessible means, such as a phone call, internet call, message on instant messengers (e.g., Google Chat, Slack), or email.

The local IT administrator is responsible for activating and enabling employees to connect the 3rd alternative internet channel and involving anyone necessary to address this task, guiding the team how.

Upon connection is established and local team is back online - notification to BCDR committee should be done via email with details about incident, recovery time. In the following emails, IT should provide also lessons learned and proposals for improvement if recovery wasn’t smooth.

#### ***Unavailability of Central Power Supply***

In the event of an unanticipated central power supply outage, the main fuel generator automatically starts supplying power to the local office.

If the main generator is not working, the following steps should be taken:

1. **Notification:** Any employee or contractor who identifies the central power supply issue must promptly inform the Asset Manager. If the Asset Manager is unavailable, immediate notification should be directed to the Chief Operating Officer (COO).
2. **Power Restoration:** The Asset Manager is responsible for initiating power restoration by activating the generator. This process should be executed in accordance with the instructions outlined in the "How to Turn On Electricity (From the Generator)" manual.
3. **Maintenance Coordination:** To ensure timely maintenance, the Asset Manager is required to communicate the generator start time to the office support team.

In the event that the central power supply is restored, the subsequent steps are as follows:

1. **Generator Deactivation:** Upon confirmation of central power supply recovery, the Asset Manager should follow the prescribed steps detailed in the "How to Switch from a Generator to Power from the City Network" manual to deactivate the generator.
2. **Maintenance Notification:** Similar to generator activation, the Asset Manager must inform the office support team about the generator deactivation time for maintenance scheduling.

By adhering to these procedures, the continuity of power supply can be effectively managed during periods of central power supply unavailability.

In the event that centralized power supply is not restored within 24 hours, we anticipate relocating teams to pre-arranged alternative locations where both centralized power supply and communication are ensured, as well as locations equipped with backup power systems and internet connectivity.

### **Terrorism attack or Increased military aggression**

Possible Scenarios:

* Missile Attacks: Sudden, high-impact events causing casualties and infrastructure damage.
* Ground Engagement: Prolonged conflict with potential for collateral damage and movement restrictions.
* Cyberattacks: Disruption of critical infrastructure and data breaches.
* Civil Unrest: Protests, demonstrations, and potential violence.

Only two main requirements are needed for the continuous provision of services to our customers: ***stable access to the Internet and employees hosted in a safe place.***

#### Technical preparedness

<Company> uses a cloud-based approach to keep up and running services and processes needed for software development and internal operations of a company. No customer data is stored or processed in Ukraine or any other country with high or critical risk.

Most of engineering and delivery team (<XX>%) is diversified and located in: USA, Canada, Poland, Spain, France,UK, Austria, Germany.

Any office separately doesn’t impact the situation as we host all data in the AWS Cloud or other cloud solutions and don’t store or process any customer data locally.

All company’s cloud-hosted resources are available via secure encrypted VPN tunnels.

The redundant VPN connections are built using at least two ISP providers and an Internal BGP routing protocol between the diversified delivery locations and AWS <Company> account (or other cloud) to grant secure encrypted access via VPN Site to Site tunnels. Access to internal company resources is also available from outside of the <City> office network via corporate SSL VPN connections.

#### Organizational preparedness

All employees and contractors can work effectively from home or any other location. After COVID-19 **<Company> is a REMOTE-FIRST company.**

All our global Offices in different locations are on rent and have enough capacity to host people from <Country> or any other location.

We prepared detailed instructions for employees and contractors with considering factors that depend on the scale and impact of this issue and, of course, it also depends on the restrictions/instructions that can be applied by the government.

On the other hand, <Company> committed to help employees/contractors and their families in case of dangerous scenarios like this.

We Continuous monitoring of the situation and notify our stakeholders and customers on any major events or changes in situations or risks escalations.

Crisis communication plan and list of responsibilities will be provided in case of this scenario.

The plans of actions for every team described within the Business Impact Analysis results.

<Screenshot with Plan of Actions>

#### ***Crisis communication plan and responsibilities for scenario «Man-made disaster, including radiation leakage / accident at a nuclear power plant»***

1. In case of receiving information about any type of man-made disaster, including radiation leakage / accident at a nuclear power plant engineer is obliged to immediately notify his PM by phone, and **the duty officer in the** <**Defined Team**> **by e-mail** and **Incident Commander** by phone (backup channel - corporate mail or chat)
2. **The duty officer in the** <**Defined Team**> must notify all members of the Crisis Management Team about the occurrence of a dangerous event according to the contact table. Crisis Management Team should perform further actions according to this plan.
3. **Incident Commander** sends out email communication templates to all employees stating they will receive instructions in the course of the next few hours. It can be duplicated in the newly created Google chat channel.
4. **Crisis Management Team** members should get in contact immediately via on-line conference meetings, phone calls, messenger applications to analyze the information and select a scenario according to the situation. The meeting is organized and managed by the Incident Commander.
5. **Incident Commander**  takes control of all other involved Teams' actions and launches approved response scenarios with clear instructions on the initial actions.
6. **The HR Team** keeps track of all contractors that might be affected, making sure everyone receives the instructions and understands what needs to be done in the course of this disaster. Updates Crisis Management Team on the overall situation every two hours. Creates the list of those immediately affected by disaster, potentially affected by disaster and not affected.
7. **PMs and Team Leads** additionally communicate with all members of their teams to confirm their receipt of the action plan, verify their availability, limitations and readiness to follow the plan. Tasks and duties are distributed among those employees, who are not affected by the disaster.
8. **The COO** is preparing to use funding reserves to cover urgent expenses
9. **Crisis Management Team** appoints responsible persons (Monitoring Team) for continuous monitoring of available information on current changes of the situation
10. **Risk Monitoring Team** submits a report on the current situation at least three times per day or immediately upon receiving an important update.
11. **IT Recovery Team** tests the availability of the primary and backup communication channels to provide continuous customer service
12. **Pre-relocated team (Remote Team)** takes responsibility for the provision of critical services to customers and communication with clients (if necessary)
13. **The Marketing Team and Sales Team** informs the company's customers about the current situation, possible risks and restrictions in providing services, approximate recovery time - according to the prepared communication map and the current situation. Keeps in touch with customers, continuously informs them about changes in the situation.
14. **Crisis Management Team** is responsible for:

* Analysis of the need to protect contractors and their families and the procedure for providing such assistance
* Re-establishing communication with out-of-contact contractors
* Analysis of available options for transporting people, if necessary
* Assist the families of contractors in ensuring their safety and allocating the necessary resources.
* Assess the existence of restrictions on crossing the borders of countries planned for relocation
* Drawing up relocation plans for groups of contractors and family members, appointing the leader of each group
* Organization of the teams' work that remains at the primary location, if available.
* Coordination of work of all other teams, change of action plans according to the development of the situation.

1. **The Finance Team**, if necessary and agreed is responsible for:

* Providing the necessary financial resources to other teams to carry out their tasks
* Providing financial assistance to contractors and their families as needed
* Organization of alternative payment options for contractors
* Monthly cash payment in the amount of monthly compensation to the families of contractors involved

1. **HR Team** is responsible for:

* Preparing contacts with contractors and their families, liaising with them and identifying needs that the business can help
* Organization of purchase and lease of necessary resources (tickets, documents, vehicles, fuel, food, water, communications, maps and schedule, etc.)
* Assistance in solving current problems during a crisis or business trip

# Testing of the Business Continuity Plan

* The reason for testing Business Continuity Plan is to simulate situations to find out the gaps during real problems.
* The Business Continuity Plan (BCP) is tested once a year - but can occur more frequently in the case of significant changes.
* Once the exercising and testing are performed, the person who coordinates business continuity reviews the result, compares them with the objectives set, and reports them to top management.

# Communication Channels

The primary corporate communication channel for calls and chats - is Google Mail/Chat.

The alternative of communication is by telephone. For Critical and High severity incidents - Phone is the primary communication channel.

For any crisis event, as described throughout this continuity plan, the following order of communication should be applied:

* Make a Call and key stakeholders notification for any critical or high severity events.
* Use Google Chat common channels to inform all team members of the situation and advise on actions (@all to trigger notifications).
* Use email to duplicate communication messages.
* HR Manager is assigned the role of Incident Commander and coordinates point-to-point communication across the team.
* The “I’m-ok” procedure is established in case of significant disaster situations, such as natural disasters. Each team member informs the Head of HR regarding their whereabouts and well-being.
* The company’s Team List is used to mark off safe team members.

Customer notification templates are available in our <CRM> for all members of BCDR Committee:

<Screenshot of Customer Notification Templates>

# Disciplinary actions

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Management will determine how severe an employee’s offense is and take the appropriate action.

# Change, Review, and Update

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by the ISMS Manager or employee that was specifically appointed to perform such a task by ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* ISO 27001 Annex A.17.1.1 Planning Information Security Continuity
* ISO 27001 Annex A.17.1.2 Implementing Information Security Continuity
* ISO 27001 Annex A.17.1.3 Verify, Review & Evaluate Information Security Continuity
* ISO 27001 Annex A.17.2.1 Availability of Information Processing Facilities

# Related Documents

* <Company> Risk Assessment
* <Company> BCP Teams and Contacts
* How to turn on electricity (from the generator) in a <Company> office
* <Company> Incident Response Plan

1. All fields in this document marked by angled brackets < > and highlighted must be filled in. [↑](#footnote-ref-0)