Wrocław University of Science and Technology
Faculty of Fundamental Problems of Technology

Information System Contingency Plan

MaliExpress

Authors

Aleksander Lasecki 236371, Grzegorz Zaborowski 236447
Paulina Jałosińska 232892, Przemek Borszowski 234869
Mikołaj Grzegrzółka 241073

Wrocław 2021

Contents

Plan Approval

As the designated authority for contingency and legal compliance, I hereby certify that the information system contingency plan (ISCP) is complete, and that the information contained in this ISCP provides an accurate representation of the application, its hardware, software, and telecommunication components. I further certify that this document identifies the criticality of the systems as they relate to the mission of MaliExpress, and that the recovery strategies identified will provide the ability to recover the system functionality in the most expedient and cost-beneficial method in keeping with levels of criticality.

I further attest that this ISCP for MaliExpress will be tested at least annually. This plan was last tested on 05.05.2021; the test, training, and exercise (TT&E) material associated with this test can be found on the company's internal website. This document will be modified as changes occur and will remain under version control, in accordance with MaliExpress's contingency planning policy.

Date

Chief Executive Officer

Information System Contingency
Plan Coordinator

Chapter 1

Introduction

Information systems are vital to **MaliExperss**'s business processes; therefore, it is critical that services provided by the organisation's systems are able to operate effectively without excessive interruption. This Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover several of these systems quickly and effectively following a service disruption. The structure of this document is as follows:

- **Chapter 1** introduces the main objectives and assumptions of the contingency plan and gives a brief look at the background, scope and structure of the document and the procedures described in it.
- **Chapter 2** gives a description of the environment and infrastructure of **MaliExpress**. It also presents an overview of the three phases of the ISCP and a list personnel along with their responsibilities.
- **Chapter 3** includes a risk analysis and assessment for each described system. The impact of each of them is assigned in accordance with FIPS 199 and provides a list of requirements (e.g. high impact systems require hot relocation sites).
- **Chapter 4** describes the Activation and Notification phase of contingency plans of each of the scenarios considered in this document. This phase is meant to prepare company personnel for carrying out recovery measures.
- **Chapter 5** describes the Recovery phase of the contingency plans of each of the scenarios considered in this document. This phase is meant to restore the capabilities of the affected system, repair damage and resume operations.
- **Chapter 6** describes the Reconstitution phase of the contingency plans of each of the scenarios considered in this document. This phase is meant to complete recovery processes, ensure that the system was properly restored and deactivate the plan.
- **Appendices** contain extra documents and tables with additional information about the company that is not essential for this plan but might be of use (especially in the Activation and Notification phase) such as personnel and vendor contact lists.

1.1 Background

This document describes Information System Contingency Plans for four chosen systems by establishing recovery and reconstitution procedures for a given disruption. The four systems/scenarios described in this document are, by no means, supposed to be considered as an exhaustive list. For contingency plans for other systems, please refer to the appropriate documents.
The following recovery plan objectives have been established:

- Maximise the effectiveness of contingency operations through an established plan that consists of the following phases:
  - **Activation and Notification phase** activates a recovery plan after a disruption or outage and determines the extent of the damage. If the event matches one of the scenarios presented in this document then the appropriate notification phase is initiated.
  - **Recovery phase** consists of a set of steps that are taken to restore the operation of the affected system as soon as possible.
  - **Reconstruction phase** ensures that the affected system is fully tested and validated. After that normal operation is resumed and the plan's execution is finalised.
- Identify the activities, resources, and procedures to carry out the processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated **MaliExperss**'s personnel and provide guidance for recovering the companies systems during prolonged periods of interruption to normal operations.
- Ensure coordination with other personnel responsible for **MaliExperss**'s contingency planning strategies. Ensure coordination with external points of contact and vendors associated with each affected system and the execution of this plan.

1.2 Scope

This ISCP has been developed for four of **MaliExperss**'s systems. The impact each of the systems is analysed in the third chapter, in accordance with Federal Information Processing Standards (FIPS) 199 – Standards for Security Categorisation of Federal Information and Information Systems. Procedures in this ISCP are appropriate for the impact of the systems and designed to recover them within a set time given as the Recovery Time Objective (RTO). This plan does not address replacement or purchase of new equipment, short-term disruptions lasting less than the given RTO, or loss of data at the onsite facility or at the user-desktop levels. Each scenario is analysed separately in accordance with its impact level and the requirements of the system in question.

1.3 Assumptions

The following assumptions were used when developing this ISCP:

- All systems have an impact level assigned in accordance with FIPS 199.
- All required alternate processing sites and offsite storage have been established for all of the systems in question.
- Backups of the systems software and data are intact and available in a location appropriate for the impact level of the system.
- Required alternate facilities have been established and are available if needed for relocation.
- A system described in this document is inoperable and cannot be recovered within the RTO.
- Key personnel have been identified and fully trained in their emergency response and recovery roles for each of the systems. They are also available for the activation of the contingency plan.

This ISCP does not apply for the following situations:

- Overall recovery and continuity of mission/business operations. The Business Continuity Plan (BCP) and Continuity of Operations Plan (COOP) address continuity of business operations.
- Emergency evacuation of personnel. The Occupant Emergency Plan (OEP) addresses employee evacuation.

Chapter 2

Concept of Operations

The Concept of Operations section provides details about **MaliExpress**, an overview of the three phases of the ISCP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of **MaliExpress**'s personnel during a contingency activation.

2.1 Environment and Infrastructure

2.1.1 Company Description

MaliExpress is a world wide internet shop specialising in electronic components and printed circuit boards. The shop is mainly targeting large electronic manufacturers (such as PC parts manufacturers) but is also open to hobbyists who work one their individual projects and prototypes. The company several private and public web servers located around the world that host two websites that allow clients to place orders and track the delivery process, the internal management system and a few smaller systems. It also owns multiple warehouses and a headquarters building which is where the management and software development teams are located. The shipment processes are handled by several delivery services:

- A global delivery company that handles inter large warehouse transportation services as well as stock import
- Multiple local delivery services that handle shipping packages from warehouses to clients within a single county.

Each delivery service is on a contract which enforces high care when handling the packages and the global service is also required to work within tight time constraints (up to 48h for a single delivery). Additionally they are required to send delivery status updates to the company's servers which allows both the company and its clients to track the shipment process.

Payments for orders are handled in three different ways to make sure this process is both secure and easy for the clients:

- For individual clients (hobbyists) all payments are processed either by a plug-in payment service provider (e.g. in Poland the service used is DotPay)
- For companies all payments are handled through direct bank transfers
- Additionally **MaliExpress** allows all of its clients to pay using a secure and private method: Bitcoin

Due to the services that **MaliExpress** provides it is necessary for the company to store several kinds of private data:

- Client's personal data such as bank account numbers, addresses, names and order logs
- Shipment information (including private parcel codes used for tracking and managing deliveries)
- Contracts and other agreements with other companies (such as delivery or payment services and product manufacturers)
- Employee's personal data such as bank account numbers, addresses, names and salaries

2.1.2 Technical Infrastructure

The technical infrastructure of **MaliExpress** consists of the following main elements:

Public web servers

The company owns a few web servers located around the world to ensure quick response times despite a possible large amount of requests and an equal treatment of all clients, no matter their location. The servers themselves are based on the latest versions of Ubuntu, Django and MariaDB. The software run on these servers is constantly updated and penetration tests are carried out periodically to ensure high levels of privacy and security and to mitigate a possibility of an attack.

Company management servers

These servers are used for internal company processes such as employee management (hiring, salary calculations and handling, etc) and task management. They are based on Ubuntu and MariaDB. Django and Node.js are also used for internal websites and services such as internal chat systems. Due to the fact that these servers hold the most sensitive data, they are given the highest priority when it comes to security testing, penetration testing as well as software updates and tests.

Warehouse management servers

These are servers local to each warehouse. They are used to quickly manage incoming import and export requests and forward them to appropriate employees. They are based on Ubuntu and a proprietary task management system written in Python.

2.2 Overview of Three Phases

This ISCP has been developed to recover the system name using a three-phased approach. This approach ensures that system recovery efforts are performed in a methodical sequence to maximise the effectiveness of the recovery effort and minimise system outage time due to errors and omissions. The three system recovery phases are:

2.2.1 Activation and Notification

Activation of the ISCP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, or other damage that typically results in long-term loss. Once the ISCP is activated, system owners and users are notified of a possible long-term outage, and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.

2.2.2 Recovery

The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system owners and users.

2.2.3 Reconstruction

The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating successful reconstitution and deactivation of the plan. During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing. Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalisation, incorporation of lessons learned into plan updates, and readying resources for any future events.

2.3 Roles and Responsibilities

The company structure is as follows:

- **Company management** - housed in the company headquarters:
  - **CEO** - The founder and owner of the company. His responsibilities are, among many others, verifying all major company decisions and processes, establishing and negotiating contracts with other companies as well as chairing the meetings of the company's boars meetings
  - **Company board** - A board of company managers which is responsible for making all major decision and establishing a plan for the companies future
  - **Human resources** - A team responsible for hiring new employees and managing those already employed
  - **Legal department** - A team of layers and other legal specialists responsible for ensuring that all company processes are in accordance with the law and that they are all well documented
  - **Infrastructure management** - A team responsible for managing all company owned warehouses and the teams working in them
- **Software development** - housed in the company headquarters and/or working remotely:
  - **General software development manager** - A person responsible for managing all software development teams
  - **Web development team** - A team responsible for developing, testing and updating all software run on public web servers
  - **Internal services development team** - A team responsible for developing, testing and updating all software run internal servers as well as warehouse servers
  - **Security team** - A team responsible for testing the security of the company code, e.g. by performing periodic penetration tests and audits
- **Warehouse management** - local to each site:
  - **Warehouse manager** - A person responsible for managing a single warehouse

- **Import team -** A team of employees responsible for handling incoming shipments
- **Export team -** A team of employees responsible for preparing and handling products that are to be sent out for delivery
- **Sorting and managing team -** The larges team of every warehouse responsible for maintain the building's infrastructure and ensuring that all product are properly sorted and stored

Chapter 3

Scenario Impact Assessment

The following chapter gives an introduction to each scenario considered in this document. It also analyses each of them in terms of impact and probability and assigns a category: **Low**, **Medium** or **High** for both of the aforementioned criteria separately. At the end, a final category is assigned for overall security.

3.1 Impact Criteria

Impact of each of the scenarios considered is analysed and evaluated based on the publication **FIPS 199** which describes each impact level in terms of three security objectives (everything in italics is a quote from FIPS 199):

1. **Confidentiality** - *A loss of confidentiality is the unauthorized disclosure of information*

2. **Integrity** - *A loss of integrity is the unauthorized modification or destruction of information*

3. **Availability** - *A loss of availability is the disruption of access to or use of information or an information system*

Based on those three objectives, the three impact levels are defined in the following way:

Low

*The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals*

Medium

*The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals*

High

*The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals*

Each of these categories has a numerical value assigned:

- **Low** - 1

- **Medium** - 2

- **High** - 3

3.2 Probability Criteria

Three levels of probability are used. They are defined in the following way:

Low

A scenario is considered to have low probability if it is **plausible but not expected** to occur.

Medium

A scenario is considered to have medium probability if it is **rare but expected** to occur after a relatively long time.

High

A scenario is considered to have high probability if it is **almost certain** to occur and it even might be expected to take place on a daily basis.

Each of these categories has a numerical value assigned:

- **Low** - 1
- **Medium** - 2
- **High** - 3

3.3 Evaluation Criteria

The final evaluation considers both impact and probability and assigns an overall security category based on the following matrix:

Probability \ Impact	**Low**	**Medium**	**High**
Low	Low	Moderate	Moderate
Medium	Moderate	Moderate	High
High	Moderate	High	High

3.4 Scenario Analysis

Finally, a brief description and analysis of each of the considered scenarios is given:

3.4.1 Payment system failure

Regarding the risk of a payment system failure, the main risk level for FIPS 199 specification will be "Availability". The damage resulting from this type of failure will arise mainly from losses caused by: a smaller number of potential orders, delaying the shipment of goods and customer satisfaction. A failure in the payment system may result in the inability to release goods for delivery without posting the payment on the account first. We can divide it into two sources of the problem: the problem with the payment system service provider (for example: bank, DotPay, PayU, etc.) and the problem with our infrastructure responsible for confirming receipt of the payment. For business partners, the available payment options are: BitCoin and direct bank transfer. In the case of BitCoin, the only thing that can fail is our system of receiving notifications about the completion of a transfer in BitCoin. A traditional transfer is handled by our bank, therefore it is responsible for the correct execution of the transfer. Due to the fact

that we are dealing with business partners with whom we settle accounts for specific settlement periods, any short bank failures affecting the speed of posting the payment on the account have negligible impact on the release of goods. In the case of individual customers, the payment is made by intermediaries such as: DotPay, PayU, etc. In the event of a breakdown at our payment system service provider (lack of availability of the entire system, failure of the notification system), the shipment of the order will be delayed until the funds are received, which may affect the number of made orders and the level of customers satisfaction. Another aspect that may fail in this case (on our side) is the system of receiving notifications about the completion of payments by an individual customer.
Impact category: **Medium**
Probability category: **Low**
Overall security category: **Moderate**

3.4.2 Credit Card Fraud

A type of fraud involving the unauthorised use of a credit card or similar payment tool such as EFT. Essentially, the process is an attempt by a potential attacker to obtain goods or services. Despite the relative security with regard to the security measures used by the sales platform. Credit Card Fraud is still a highly dangerous attack that can affect the vital structures of the entire store. The issue related to the harmfulness of such an attack depends on its scale. For example, potential attacks of this category may target specific, most expensive goods offered by a company or be a serious sequence of attacks carried out over time. For a better understanding of the problem and possible losses, the characterisation of this kind of attacks should be introduced. There are two basic types of this type of fraud, Card-Present fraud and Card-Not-Present fraud (currently more popular). Depending on the situation related to the attack, we must expect a situation in which someone will try to set up an account with the data of another customer and charge the victim with the actual value of the purchased goods. It is also possible to hijack someone's account in the standard way or by using hacking techniques. With regard to the risk resulting from Credit Card Fraud, the main levels at risk in relation to the FIPS 199 specification will be "Availability", and additionally "Confidentiality". Damage resulting from this type of attack will mainly occur in relation to material losses incurred by the online store. This can cause serious problems in the overall functioning of the sales platform, not only due to damage to its operating mechanisms, but also due to the overall confusion it causes. In addition, the threat to "Confidentiality" will result from the potential method of implementing such an attack. The sensitive information stolen by the attacker and used in the fraudulent process may simply spread. When analysing the structure of the sales platform, we can also expect a situation related to an unnoticed charge-back, despite the product being acquired by the buyer. In such a situation, the customer may receive the entire amount of the payment, despite having the purchased goods. In addition, with this method of attack, we must expect that the sales system will not register the use of a stolen and / or blocked credit card or other payment identifier.
Impact category: **Medium**
Probability category: **High**
Overall security category: **High**

3.4.3 Power failure

Power outages can be caused by a number of factors, including storms, trees, human error, vehicles, animal interference, repairs and more. Taking into consideration that MaliExpress, like most companies in today's world, will rely on electricity every day, a power outage will have consequences. The issue related to the harmfulness of such event depends on the timing of the outages. When analysing the impact of power cuts, three time windows can be distinguished. The first time window covers the period when the store is closed for both employees and customers, i.e. during the nights and on public holidays.The second case occurs when the store is closed for customers, but the employees are cleaning up or inventorying. The last and most complicated case takes place during the opening hours of the store for customers. This situation is associated with lower revenues as stationary customers will choose

to purchase from the competition. In every case of power outages, the security systems in the store, i.e. cameras and motion sensors(if there is no one in the store), switch to emergency power. Emergency power is associated with additional costs for the company. When the emergency power is exhausted, the store will no longer be protected by security systems, which will increase the chances of a successful break-in.
Impact category: **Medium**
Probability category: **Low**
Overall security category: **Moderate**

3.4.4 Warehouse fire

Fire in the warehouse might occur due to many factors, such as misuse of the electronic devices, ligthning, arsons and even vehicle fuel leaks. The damage of will depend on fire range, succesful evacuation and established security of area after the incident. It is important to notice that fire in the warehouse might affect merchandise, servers and potential casualties. Security systems will detect fire through smoke sensors, however alarm could also be raised by a person inside the warehouse. This could create an opportunity to begin plan immediately. Not always there will be enough staff to explore all parts of the building. so time fire comes might change a lot in the scenario. During the nights, fire might be much more difficult to stop. In any case, the staff must be aware of evacuation procedure. When alarm is raised, fire brigade will make every effort to minimise the damage caused by fire. When the fire stops, the warehouse might need to temporarily raise the security level in order to prevent any theft or further damage to the infrastructure.
Impact category: **High**
Probability category: **Low**
Overall security category: **Moderate**

Chapter 4

Activation and Notification

The Activation and Notification Phase defines initial actions taken once a disruption of one of the systems has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the ISCP. At the completion of the Activation and Notification Phase, ISCP staff will be prepared to perform recovery measures.

4.1 Payment system failure

4.1.1 Activation Criteria and Procedure

The Payment system failure ISCP may be activated if one or more of the following criteria are met:

1. information from the service provider of the payment system about the failure or planned interruptions in the provision of services,

2. information from the server supplier about a failure, planned interruptions in the supply of services or other problems,

3. information from own teams (the Internal services development team or the Web development team) about the detection of failures or other indications of a possible incorrect functioning of the system,

4. numerous problems reported by other employees or clients (initially verified as to their validity by the Internal services team and the Web team).

When a failure is detected or such information is received the General software development manager may activate the ISCP.

4.1.2 Notification

The first step upon activation of the Payment system failure ISCP is notification of appropriate personnel. The General software development manager should immediately contact with the Internal services development team to begin preliminary work to determine the cause of the failure and whether the failure persists. Based on the first findings, such as whether the problem persists, the General software development manager should decide whether the Web development team should be notified of the problem. The Web development team in some situations may be needed to inform customers about temporary payment problems, disable specific payment methods temporarily, etc. The method of notification should be chosen one that will allow the necessary teams to be notified as soon as possible (preferably by phone call) and to determine the most convenient way of further communication for the purpose of solving the problem (for example Microsoft Teams).

4.1.3 Outage Assessment

Upon notification, a thorough downtime assessment is required to determine the cause of the problem, extent of the disruption, possible damage, and estimated recovery time. This downtime assessment is carried out by the General software development manager in conjunction with the Internal services development team. The failure assessment procedures depend on the criterion that contributed to the activation of the Payment system failure ISCP. If the problem happened with one of our partners, the first thing you should do is contact them to clarify the problems: what are the problems, when will they stop, what systems was it affected by, when the first problems occurred, etc. All such information may be needed for outage assessment and estimated time to restore service to normal operations. If the failure is related to our infrastructure or the cause of it is unknown, an internal analysis should be carried out as soon as possible to find the potential reason for the failure. Once the cause of the failure is established, you can proceed with the repair plan and estimate the time needed to restore the system functionality (you may need to contact our partner(s) to find/solve the problem).

4.2 Credit Card Fraud

4.2.1 Activation Criteria and Procedure

If a card fraud is confirmed, the company's security team and the Company Board are immediately informed. The primary activity carried out is that the lead supervisory team liaises with the card issuer's authorization center on the transaction being performed (”code 10 authorization request”). In addition, during the Activation and Notification phase, estimates related to losses resulting from the existing Card Fraud are determined. In the course of the operation stage, the deceived client is not confronted with the fraud. During the cooperation with the authorization center of the card issuer, the police are also informed about the occurrence of the presented type of fraud.

4.2.2 Notification

For each confirmed Card Credit Fraud, it is necessary to notify the relevant structures responsible for managing the company's financial resources. Additionally, the security team must be notified in order to identify the source used in the attack, and the management in the procedure of determining potential involvement in the attack within the company's internal structure.

4.2.3 Outage Assessment

In general, the whole situation depends on the characteristics of the attack performed. The form of such an attack is probable and very popular, so teams are prepared to deal with damage and implement repair processes. The exact implementation of the process of finding the perpetrator of an attack depends in most cases on the participation and effectiveness of police units.

4.3 Power Failure

4.3.1 Activation Criteria and Procedure

At the beginning, the employees must check whether what looks like a power failure is not a failure of devices that require electricity, such as a surge protector, light bulbs, light switch. In some situations more then one device breaks down at the same time. If this is a problem, the employees should replace, if possible and safe for them, the damaged devices and return to normal operation. If the devices can not be easily replaced, the call to specialists, who repair this type of failures must be made as fast as possible.

4.3.2 Notification

Whenever the power failure is confirmed, the phone call to electricity supplier must be made. If the cause if power failure will happen to be an internal problem, call to specialists who repair this type of failures must be made as fast as possible. When analyzing the impact of power cuts, as it was said in chapter tree, three time windows can be distinguished. The first time window covers the period when the store is closed for both employees and customers, i.e. during the nights and on public holidays. In this case, the security systems in the store, i.e. cameras and motion sensors, switch to emergency power. The second case occurs when the store is closed for customers, but the employees are cleaning up or inventorying. In this case, cameras must switch to emergency power, which involves additional costs. Additionally, employees will either be released home early or continue working with flashlights and other light sources. Both solutions involve additional costs for the employer. The last and most complicated case takes place during the opening hours of the store for customers. If a power outage is planned through repairs, employees may announce store closures with proper notice. Customers who shop online can still be served as long as employees will work on laptops. Flashlights and other light sources will also be necessary. In the case of desktop computers, it is also possible to provide backup power, but it costs more than backup power for laptops. In a situation where there are customers in the store, employees must lead them safely outside the store (if there is no access to external light, use flashlights).

4.3.3 Outage Assessment

When the appropriate services arrive to rectify the cause of the failure, a thorough downtime assessment is required initially to determine the cause of the problem and possible damage. Apart from damaged elements or devices, it is necessary to inspect all electrical installations, electrical sockets, etc. in the store. Once the cause of the failure is established, they can proceed with the repair plan and estimate the time needed to restore the system functionality.

4.4 Warehouse fire

4.4.1 Activation Criteria and Procedure

Fire emergency is activated by either automated smoke detector or a person who perceives a dangerous fire. The actual activation start by either a person raising an alarm or security officer when the alarm comes from a detector. When the fire is too severe to extinguished by an individual or it is too late to reach before it spreads, the fire brigade must be called immediately.

4.4.2 Notification

In any case of fire, smoke detectors should activate the alarm, however the alarm may also be raised by a person by activating one of the alarm switches. Then, a person from security team must call fire department immediately. The process of evacuation should start right after the alarm starts. Everyone should exit the building through evacuation route. Without running and with everyone staying on the line. By the time fire brigade arrives, everyone should escape the building. In any other case, the brigade should be informed.

4.4.3 Outage Assessment

Fire Brigade knows how to handle a situation. All they need to know is whether there are any people left in the building. After the fire is stopped, the warehouse might still be vulnerable. Local security team should call Chief Security Officer to check the situation. After the proper assessment CSO should know if the warehouse needs any reinforcement to protect the place. There is also a matter of servers in the warehouse. This should be easily checked by one of the technicians. If the fire damaged the hardware or the servers are unavailable, they should call the infrastructure management.

Chapter 5

Recovery

The Recovery Phase provides formal recovery operations that begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilised. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the Recovery Phase, the system that experienced a disruption will be functional and capable of performing the functions identified in **Chapter 3** of this document.

5.1 Payment system failure

5.1.1 Sequence of Recovery Activities

The following activities occur during recovery of the payment system failure.

- If the failure occurred with one of our partners:
    1. Posting information about possible problems with the payment (if still occurs).
    2. Blocking the non-functioning payment method (if required and still occurs).
    3. Working with a partner to fix the problem (if required).
    4. Waiting for the failure to be fixed/ceased.
    5. Restoring the blocked payment method (if blocked) and removing the message about problems (if published).
    6. Verification of all orders/payments that have been made from the start of the failure to its cessation (or until the payment method has been blocked).
- If the failure occurred on the side of our system (e.g. the system of receiving notifications):
    1. Posting information about possible problems with the payment (if still occurs).
    2. Starting a fallback server (if applicable).
    3. Identification of the problem and the resources needed to complete the recovery procedure.
    4. Realization of works aimed at restoring the functioning of the system.
    5. Removing the message about problems (if published), deactive fallback server (if applicable).
    6. Verification of all orders/payments that have been made from the start of the failure to its cessation.
    7. Verification of performed activities and analysis of preventing the occurrence of a problem in the future.

5.1.2 Recovery Procedures

The general software development manager oversees the work of all teams involved. He is also a decision-maker whose competence lies in solving the problem as quickly and as good as possible. He is also responsible for the possible contact with business partners or the appointment of persons responsible for it. If The Web development team is needed, it is responsible for informing customers about the failure and blocking selected payment methods. The internal service development team is responsible for identifying the cause of the failure. If applicable, the internal service development team is responsible for running and monitoring the fallback server. If required, the internal service development team works with business partners to resolve an existing problem. If it is a failure on our side of the system, the internal service development team must identify the cause of the failure and determine the measures and actions needed to resolve the problem, then proceed to repair the system. After restoring the functionality of the payment system, the Web development team removes the information about the failure of the payment system (and unblocks selected blocked payment methods) and the internal service development team starts to verify orders/payments made while the payment system did not work properly. If the failure was caused on our side of the system, the general software development manager, the internal service development team and other persons who may be of importance for the case, organize a meeting(s) to discuss and analyze the actions taken to eliminate the failure and analyze what steps should be taken to minimize the occurrence of a similar failure in the future. The Web development team may be involved in additional activities (appointed by the general software development manager) if this can help in a faster system recovery.

5.1.3 Recovery Escalation Notices/Awareness

The general software development manager, as a decision-making person through whom all important information passes, is obliged to inform the CEO about the failure and any progress related to failure identification and the course of its repairs, e.g. by e-mail. The general software development manager may delegate a selected person to this task, provided that they have access to the necessary information. All teams involved in the repair of a failure can conduct a direct exchange of information (acquired knowledge) with each other in order to accelerate the process. It is worth emphasizing, however, that each action taken by the team must be previously reported to the general software development manager (e.g. the need to shut down and restart the server). Any conflicts between teams or team members should be promptly consulted with team leaders who should discuss the issue with the general software development manager in case of further doubts.

5.2 Credit Card Fraud

5.2.1 Sequence of Recovery Activities

The operation sequence in the case of Credit Card Fraud is as follows:

1. Informing the management structure, security team and human resources of the company,
2. Checking whether the company's employees participated passively or actively in the attack,
3. Identification of how the attack was carried out,
4. Immediate validation whether a complete change of credit cards is necessary or a possible diversification of the payment methods used,
5. Decision if the functionality of company's store should be suspended or not,
6. Loss analysis and report for the distribution of company funds,
7. Implementation of the procedure for managing the company's finances, taking into account the losses incurred,

8. Then the marketing team deals with the renewal of the company's image.

5.2.2 Recovery Procedures

The next phase is the process of quickly recovering from the Card Fraud. One of the basic steps is to check the possible responsibility of someone from the company's employees in breach. In this case, top management and Human Resources are involved in the procedure to take appropriate disciplinary action. Depending on the type of attack or losses suffered, the functionality of the company's store is temporarily suspended until new credit cards are obtained, if the actual cause of the attack lies with the attacker's gaining access to the company's credit cards. Additionally, an analysis of the damage caused is performed in order to implement the procedure of segregating the company's financial distributions. Subsequently, key steps are taken by the security department to establish the exact source used during the attack. Then, the management team responsible for the company's image estimates the potential damage caused to the company's reputation and customer relations. People responsible for repairing the company's image in the sphere of contacts with customers and partners are appointed.

5.2.3 Recovery Escalation Notices/Awareness

An important issue in the initial phase is the verification of potential sources of information leakage. Therefore, basic information about the incident is provided only through a structure that actively uses the functionalities of payment systems. An important issue is not the aggrieved client's involvement in the entire procedure, only immediate reaction and potential compensation.

5.3 Power Failure

5.3.1 Sequence of Recovery Activities

In case of power failure a sequence of activities must be performed:

1. Informing those present in the store about the power failure,
2. finding spare light sources by employees.
3. Customers evacuating (if there are any present).
4. Making a phone call to the power supplier.
5. Making a phone call to the service repairing the power failure.
6. Delegating an employee to cooperate with the services.
7. Waiting for arrival of the services and investigation.
8. Returning to work (if possible), after the services arrive and confirm it is safe to work.
9. Connecting devices to backup power sources (if it does not happen automatically).

5.3.2 Recovery Procedures

After preparing the shop to arrival of service technicians (after customers evacuation and choosing a person who will work with technicians) the employees must wait in a safe place and do not do any work. They can come back to work after investigation of the failure and confirmation that it is safe to work. After a power outage investigation has been completed the repairs also can start. At the same time the website administrator can post a relevant statement to customers with an apology and explanation of the matter. If the cause of the power failure was internal, the installations should be adequately secured or replaced if the fault resulted from an old infrastructure.

5.3.3 Recovery Escalation Notices/Awareness

An employee delegated to help is to inform about the course of work and provide the required information to the services (the manager may delegate himself). Communication between workers working in different rooms should be limited in order to avoid accidents (e.g. stumbling in low light) and unnecessary chaos. The services must have a space to work, so repairs could be completed as quickly as possible.

5.4 Warehouse fire

5.4.1 Sequence of Recovery Activities

In case of fire a sequence of activities must be performed:

1. Fire must be set either by an smoke detector or a person nearby
2. people inside the building start evacuating
3. A person in local security decides whether to call a fire department
4. A fire department arrives and start extinguishing the fire
5. During that time, Chief Security Officer should be called. He will probably arrive after the fire is stopped.
6. CSO checks if the building needs security reinforcements
7. Local workers check how many of the products were destroyed in the incident
8. Destroyed products should be ordered to regain stock
9. On hardware side there should be a technician checking on any problems with the servers. Any problems should be reported to the technology department of the company
10. Using data backups the servers should be restored in a while.

5.4.2 Recovery Procedures

When fire department puts out the fire, all employees should be evacuated and staying in a safe distance from the building. They can come back into the building only after the clear sign that there's no danger anymore. Later the employees might start the assessment in the warehouse by gathering data about potential damage caused by fire.

5.4.3 Recovery Escalation Notices/Awareness

Warehouse manager with the help of employees gathers all the data about product loss during the fire. Personnel should be assigned to specified sectors of the warehouse in order to gather information properly. Eventually all the information about both products and server condition should be available to CEO.

Chapter 6

Reconstitution

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone significant change and will require reassessment and reauthorisation. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

6.1 Payment system failure

6.1.1 Validation Data Testing

The internal service development team under the supervision of the general software development manager is responsible for the reconstruction of money transfer data (the time from the failure occurrence to the end of the failure). The data is reconstructed on the basis of the data provided by the payment service provider(s). This can be manual or automatic/semi-automatic process, depending on the means provided by the payment service provider(s). The general software development manager is obligated to check that all data has been reconstructed and to prepare a detailed report (including data values before and after reconstruction).

6.1.2 Validation Functionality Testing

The internal service development team supervised by the general software development manager is responsible for restoring full functionality after a failure. For the correct operation of the system to be approved, it must pass all unit and automatic tests. The general software development manager is obliged to check whether all tests have passed and whether they have been performed properly. Tests are always performed on the development server, except for situations where, for some reasons, they must be performed on the production server (then external network traffic must be blocked on the production server).

6.1.3 Recovery Declaration

Upon successfully completing testing and validation, the general software development manager, will formally declare recovery efforts complete, and that the payment system is in normal operations. In addition, the ISCP coordinator will notify all teams working on the failure and the CEO about it.

6.1.4 Notifying Users

After the payment system returns to normal operation, the general software development manager will notify regular employees that the failure has ceased (broadcast message) and ask the Web development team to remove the failure information from the website (if applicable).

6.1.5 Cleanup

During the cleanup process, the internal service development team deactivates fallback server (if used). The Web development team should remove the failure information from the website (if not done). All persons who had access to confidential data provided by the payment service provider in order to reconstruct the payment data from the period when the failure occurred and ceased, are obliged to destroy/delete them (the exception is the data needed to prepare the report, in this case it must be deleted after preparation report). The general software development manager organizes a meeting (for teams representatives) to consider what steps should be taken to minimize the likelihood of a similar failure in the future.

6.1.6 Data Backup

Backups are performed on an ongoing basis, but an additional backup should be made and placed on the server that stores the backups.

6.1.7 Event Documentation

The general software development manager as a decision-maker and supervisor of the entire process is obliged to prepare detailed documentation. As the person through whom all information passes and approves all activities, he has all the information needed to prepare a proper report. Additionally, each team participating in the failure is obliged to keep its own report with a record of: activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities), functionality and data testing results, documentation of lessons learned and any additional comments. The general software development manager, based on reports from other teams and the data collected by him, prepares a summary report and delivers it to the CEO. The general software development manager, in case of any doubts, may ask other teams for additional documents and clarifications.

6.1.8 Deactivation

Once all activities have been completed and documentation has been made, the general software development manager will formally deactivate the ISCP recovery and reconstitution effort, then report is sent to CEO.

6.2 Credit Card Fraud

6.2.1 Validation Data Testing

In the event of a Credit Card Fraud attack, the credit cards used by the company may be breached and the data used in payment processes may be at risk. In addition, sensitive personal data may be used if the attack was impersonated by their use.

6.2.2 Validation Functionality Testing

Store operation is restored with validation of the credit cards and payment methods used. The potential loss of data confidence resulting from the undergrowth is implemented based on the actions of the management and the team responsible for marketing and human resources management.

6.2.3 Recovery Declaration

Restoring the procedure for the operation of payment systems is based on the verification of the attack characteristics and the potential losses resulting from it. Therefore, the process of re-running all sales procedures may depend on the operation of the banking procedure related to the transfer of new credit cards. Additional recovery processes are taken care of in order to speed up the entire procedure, however, here the potential time of their execution also depends on the scale of the attack.

6.2.4 Notifying Users

In this case, only the necessary people responsible for security as well as management and the HR department are notified in order to potentially detect the involvement of employees from the internal structure of the company in the attack. The injured customer himself is not immediately informed immediately. It is not desirable to involve the client in the potential losses resulting from the attack.

6.2.5 Cleanup

In the cleanup process, all services of the payment system are restored. Depending on the involvement of the company's employee, the attack involves a thorough expertise related to possible omissions and the procedures for checking the company's employees. In addition, the security team checks the system vulnerabilities used in the attack.

6.2.6 Offsite Data Storage

Access to information related to payment procedures and customer data of the company is available, although there is a significant reduction in people having access to it for the time of thorough verification of the attack.

6.2.7 Data Backup

All data related to clients experiencing an attack is secured with regard to the highest confidentiality of information. Additional procedures for securing payment information are implemented by the security team.

6.2.8 Event Documentation

Usually depending on the situation and the possible involvement of the company's employees in the attack. Expert opinions are prepared on the very characteristics of the attack, the exact data of the people involved and the company's sectors. In addition, a separate report is prepared by the security team related to the detected vulnerability in the payment system, or the information distribution procedure within the company. An additional report is prepared by the marketing team regarding the potential losses incurred on the good name of the company.

6.2.9 Deactivation

During the implementation of repair processes and the preparation of protocols, if the full effectiveness of the actions carried out is confirmed, the full operation of the online store and the payment system is resumed. Depending on the detected defects or the potential involvement of the company's employees in the attack, appropriate security procedures are imposed that may delay the resumption of operations or the circulation of important information within the company's structure.

6.3 Power failure

6.3.1 Validation Data Testing

In the case of power failure there is a need to check if temporary data was corrupted as the consequence of a sudden shutdown of the desktop computers. The power cut can not cause a data damage at any other stage.

6.3.2 Validation Functionality Testing

The service technician team is responsible for restoring full functionality after a failure. After all repairs, service technicians and the the delegated employees should personally check is all devices work correctly before starting normal work, especially electric devices (they might cause danger if not working correctly).

6.3.3 Recovery Declaration

Electrical and electronic devices should work normally after being connected to the power supply as soon as the fault is corrected. The only data that could be lost or damaged is temporary data that has not yet been saved. There is no possibility of recovery.

6.3.4 Notifying Users

Power failure repair services should inform the manager about the cause, exact location of the problems and how it was resolved. It should be presented what actions were finally taken and whether the failure could be a threat to the life and health of employees.

6.3.5 Cleanup

When the problem will be resolved,the shop must be prepared for another power outage.The necessary step is to recharge the backup source of energy (or buy new ones, if the old are not enough). It should be considered whether the failure could be avoided because its cause was the result due to carelessness or lack of proper training of employees.

6.3.6 Offsite Data Storage

It is possible to use offsite data storage during a power cut. Access to data is possible because it is computers are connected to a backup power source.

6.3.7 Data Backup

During a power outage and at any other time, access to data is possible because it is stored on the cloud or on hard drives that can be read as the computers are connected to a backup power source.

6.3.8 Event Documentation

Two separate protocols regarding the incident must be drawn up by the service technicians and by the store employee (manager or a designated person). Protocols may be needed when claiming compensation from an insurance company.

6.3.9 Deactivation

After the protocols are drawn up, proper notice regarding the resumption of the store's opening for the stationary clients should be placed on the door and website.

6.4 Warehouse fire

6.4.1 Validation Data Testing

During the incident warehouse hardware might be damaged, so there will be need to ensure that the recovered servers are working correctly.

6.4.2 Validation Functionality Testing

Team of technicians should check whether all systems are ready to start functioning again. After exchanging every potentially damaged hardware, there is a little chance that not everything was installed correctly.

6.4.3 Recovery Declaration

Every data collected in the servers should have a cloud backup storaged. A proper recovery might be needed

6.4.4 Notifying Users

Fire might damage products which were still counted as available. This means that the company should contact some clients about potential delay of their shipments and offer a chance to resign if the client wouldn't be interested in buying the product anymore.

6.4.5 Cleanup

In case of fire, cleanup is the most important part of the process. Every piece of equipment lost due to the incident should be documented and restocked as soon as possible. Many parts of building might also be unusable the storage will have to be planned in some other way. Rebuilding specific parts of the infrastructure will probably take some time, however with increased security, everything should still work as intended.

6.4.6 Offsite Data Storage

During the process, cloud backup data might be used to put the servers up again.

6.4.7 Data Backup

All data storaged on the warehouse server should have a cloud backup, which will help in the reconstitution.

6.4.8 Event Documentation

Warehouse manager is responsible for making a full documentation of the event and being in touch contact with CEO of the company.

6.4.9 Deactivation

When performing all of the activities, the warehouse might start working properly and the ISCP can be deactivated.

Chapter 7

Appendices

7.1 Personnel Contact List

The following list should be filled in with emergency contact information

Key Personnel Contact List	
Position	**Contact Information**
CEO	
HR Manager	
Legal department manager	
Infrastructure manager	
General software development manager	
Warehouse manager	

7.2 Vendor Contact List

The following list should be filled in with emergency contact information

Vendor Contact List	
Vendor Name	**Contact Information**