**Author:** *Alessandro Ferro*

**ICTSAS505**

**Task 3**

**PART 2**

IT Disaster

Recovery Plan:

Online System Solutions –

Web Hosting Services

|  |  |  |  |
| --- | --- | --- | --- |
| **REVISION** | **DATE** | **NAME** | **DESCRIPTION** |
| 1.0 | 25/08/2020 | Alessandro Ferro | First draft |
|  |  |  |  |
|  |  |  |  |

1.Company Profile

Online Systems Solutions is a small company that just recently started to offer web hosting services. The quick growth experienced by the company required to allocate existing and new resources and spaces to web hosting and therefore to revisit and review thhe disaster recovery procedures in place, if any.

The company relies on an office space for administration, IT infrastructure and related staff, but utilises a virtual office to coordinate and manage the staff that work remotely from various location around the world.

2.Objectives and Overview

The purpose of this document is to offer a detailed view of the risks associated with the Online Systems Solution business, reporting on their impact and describing the most effective measures to prevent, respond to and recover from in the eventuality a disaster happens.

By disaster is intended any event that disrupts the normal business operations (for more see Section 10).

Furthermore the document specify the procedures and the criteria to declare a disaster and to update and to test the plan itself.

3.Business Processes

The business is comprised of an administration section that handles payroll, finance and scheduling and an IT infrastructure section that manage and maintain the hardware and software that allow the company to operate. Both the section work from the allocated office.

The services that represent the product offered on the market by the company are managed by remote staff that coordinate and commmunicate through a virtual office.

The disruption of one or more of this processes would impact the operativity of the company, with the potential of causing major financial loss.

4.Risks

This section highlights the risks the company is subject to. The risks are divided in two categories: Physical and Electronic.

Physical risks are those that affect the hardware or material properties of the business. They can include Natural calamities such as tornadoes or floods, fire, earthquakes etc. Other risks that fall under this category are those ones less evident but that can still cause major damage, such as water leakage, huidity, overheat, etc.

The Electronic risk category comprises all the human activities that either unintentionally, or with malicious intent, can compromise the security and health of an IT system. Examples of Electronic risks are hackers, virus, cyber criminals, etc.

Upon analysis of the circumstances in which Online Systems Solutions operates, it as been noticed that the company is subject to both physical and electronic risks and that the measures in place to protect the company in case of an emergency are lacking or insufficient when they exist.

5.Analysis of Risks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Impact on Hardware** | **Impact on Software** | **Impact on Data** | **Notes** |
| **Fire** | Heat damage,  Smoke damage,  Explosion,  Building collapse | Corruption of media | Loss | Can cause huge financial loss |
| **Flood** | Water damage,  Destruction | Corruption of media | Loss | Will vary in severity |
| **Humidity** | Damage | Corruption of media | Loss | Risk increases if not detected timely |
| **Water Leakage** | Water damage,  Corrosion | Corruption of media | Loss | Risk increases if not detected timely |
| **Telecommunications and Power Outage** | Possible damage | Corruption of media | Loss | Impact depends on downtime |
| **Hardware/Software Failure** | Possible damage | Corruption of media | Loss | Will vary in severity |
| **Hackers** | Possible damage | Corruption of media | Loss, theft | Will vary in severity according to motivation |
| **Virus** | Possible damage | Corruption of media | Loss | Will vary in severity |
| **Sabotage and Terrorism** | Destruction of property | Corruption of media,  theft | Loss, Corruption, theft | Will vary in severity |

6.Prioritisation of Risks & Rationale

**Likelihood ranking**

1. Highly unlikely
2. Quite unlikely
3. Possible
4. Quite likely
5. High likely

**Impact ranking**

1. Low impact
2. Mild impact
3. Severe impact
4. Critical impact

|  |  |  |  |
| --- | --- | --- | --- |
| **RISK** | **LIKELIHOOD** | **IMPACT** | **RATIONALE** |
| **Fire** | 3 | 4 | A fire escape path is the only fire emergency measure currently mentioned |
| **Flood** | 3 | 4 | The building houses three business, meaning it is probably low raise. |
| **Humidity** | 5 | 3 | Server room 1 has no emergency measures for power outs.  Server room 2 has no air conditioning |
| **Water Leakage** | 3 | 3 | The entirety of the assets of the company relies on electricity to operate. There is no mention of water leakage detection systems. |
| **Telecommunications and Power Outage** | 4 | 4 | A UPS with 30 minutes supply exists, but only for server room 1. |
| **Hardware/Software Failure** | 5 | 4 | Measures currently adopted are vague, undocumented and untested.  There si no properly allocated space for data backup. |
| **Hackers** | 4 | 4 | Access to server rooms is granted to too many people.  Laptop allocated to remote staff have full access to the system and are not exclusively dedicated to company’s business |
| **Virus** | 4 | 4 |
| **Sabotage and Terrorism** | 4 | 4 |

7.Disaster Prevention

The following table proposes some options to prevent and minimise the risks identified and analysed in the previous sections.

|  |  |
| --- | --- |
| **Fire** | Detection systems:   * Smoke detectors * Fire alarms   Suppression systems:   * Automatic fire suppression systems * Fire hose reels * Fire hydrants * Fire extinguishers * Fire drenchers   Safety measures:   * Fire doors * Solid-core doors * Exit signs * Emergency lighting |
| **Flood** |  |
| **Humidity** | Server room 1:   * Adoption of a strategy to manage power outages (more about it in the power outage section)   Server room 2:   * Installation of an air conditioner |
| **Water Leakage** | * Water leakage monitoring and detection system |
| **Telecommunications and Power Outage** | * UPS in server room 1   Alternatives and suggestions:   * Stand-by generators * Surge arrestors |
| **Hardware/Software Failure** | * Cloud or Hybrid cloud data backup storage * Data backup location different from business location * Data backup location secured |
| **Hackers** | Protection from physical intrusion:   * Surveillance outside of working hours * Restrict access to server rooms only to staff members that need it * Lock server room 1 * Card scan with card access   Protection of IT systems:   * Restrict laptop allocated to remote staff to work use only. |
| **Virus** |
| **Sabotage and Terrorism** |

8.Disaster Response

When an incident occurs a disaster response team should be activated to assess the extent of the emergency and decide the course of action. Considering that a good portion of the personnel works remotely, the disaster response team will consist of the administration and IT staff that operate from the business facilities.

It is the disaster response team to call the emergency services if they are needed.

Other responsibilities of the disaster response team include:

* Assess how and how much the business has been affected by the disaster
* Decide which elemnt of the disaster recovery plan should be activated
* Implement measures to return to normal operations
* Notify all the emplyees

The company relies on a propietary virtual office solution to operate their software development business and to in-house servers for their web hosting services.

In the event of a disaster, should every prevention measure taken fail, the entirety of the busness IT infrastructure could collapse, causing major losses and potentially leading to the closure of the business itself.

To guarantee business continuity in case of disaster, the company should adopt a response strategy that would prove efficient as well as cost effective.

Considered the size and current situation of the business, the first reccomendation would be to dedicate the remanining capacity of the servers in room 2 to implement a Warm/Cold Stanby strategy. The servers allocated would have a copy of the IT infrastructure necessary to the company to operate, thus allowing to set up and recover full business operations with losses as minimal as possible.

In alternative, considering that the business is growing and it could be in the company interest to dedicate the entirety of their servers space to produce revenue, the Warm/Cold Stanby option could be purchased from a third party company.

It is also worthy of consideration that the currently used propietary virtual office software could be replaced by a different solution from a software service provider.

9.Disaster Recovery

In this section are specified the processes pertaining the recovery from a disaster.

Similarly as for disaster response, disaster recovery requires a team to take action to carry out the procedures related to recover when a disaster happens.

This disaster recovery plan relies on the resources already availbale to the compnay. All the hardware, software and the people workinng in the company are sufficient to undertake the tasks proposed.

If the use of any additional resource is suggested, it is specified on the procedure itself.

|  |
| --- |
| **Backup Procedure** |
| **Author:** Alessandro Ferro  **Date Created:** 27/08/2020  **Version:** 1.0  **Scope:** Data backup on the servers in the server room 1 and server room 2 located in the Online Systems Solution physical office.   |  |  |  | | --- | --- | --- | | **Task** | **Responsible Person** | **Time** | | Perform a full backup of the data of the web hosting platform. | Manager of IT services | Daily after business hours |   **Suggested additional resources:** Offsite data storage.  **Signed by author:**  **Signed for approval:** |

|  |
| --- |
| **Premises Security Procedure** |
| **Author:** Alessandro Ferro  **Date Created:** 27/08/2020  **Scope:** To ensure that the premises are not accessed by unauthorized persons   |  |  |  | | --- | --- | --- | | **Task** | **Responsible Person** | **Time** | | Always lock the door to server room 2 when no personnel is inside.  Lock the door the both server rooms outside of business hours. | Manager of IT services | Daily |   **Suggested additional resources:** Card scan would grant card access only to authorized prsonnel  **Signed by author:**  **Signed for approval:** |

|  |
| --- |
| **Data and System Security Procedure** |
| **Author:** Alessandro Ferro  **Date Created:** 27/08/2020  **Scope:** Protect the company software and data from malicious attacks   |  |  |  | | --- | --- | --- | | **Task** | **Responsible Person** | **Time** | | Configure Firewall  Set up anti virus software  Implement authentication measures | Manager of IT services | For every change and update. |   **Signed by author:**  **Signed for approval:** |

|  |
| --- |
| **Warm/Cold standby activation Procedure** |
| **Author:** Alessandro Ferro  **Date Created:** 27/08/2020  **Scope:** Ensure continuity of business operations in the event of a disaster.   |  |  |  | | --- | --- | --- | | **Task** | **Responsible Person** | **Time** | | Recover data backup to secondary server.  Adjust network configurations to point to secondary server.  Activate application software on secondary server. | Manager of IT services | In case of system critical failure |   **Signed by author:**  **Signed for approval:** |

|  |
| --- |
| **Response to Intrusion Procedure** |
| **Author:** Alessandro Ferro  **Date Created:** 27/08/2020  **Scope:** To safeguard the company’s data and software in case of an external intrusion in the system   |  |  |  | | --- | --- | --- | | **Task** | **Responsible Person** | **Time** | | Identify the breach  Contain the breach (Disconnect affected devices from the internet).  Warm/Cold standby activation  Review remote access protocols  Change all user and adinistrative credentials  Remove the cause of the intrusion and patch and update the system. | Manager of IT services | In case of system critical failure |   **Signed by author:**  **Signed for approval:** |

10.Declaring a Disaster

The following table tries to define the level of an hazard or disastrous event and to provide a mean to accordingly assess the most appropriate course of action.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Disaster Classification** | | | | |
| **System** | **Classification** | **Relevant Procedures** | **Responsibility to declare** | **Responsibility to coordinate** |
| Fire | Level 1E | Data backup and recovery.  Premises security.  Emergency response. | Automatically notified by fire alarm. | Manager of facilities. |
| Hardware/ Software Failure | Level 2H | Data backup and recovery  Warm/Cold standby activation | Manager of IT services | Manager of IT services |
| Hacker/Virus/ Sabotage and Terrorism | Level 1H | Data and systems security.  Response to intrusions. | Manager of IT services | Manager of IT services |

Clasification levels:

Level 1H - Level 1 Hazard: A hazard with high level of impact on critical business processes. Response must be immediate.

• Level 2H - Level 2 Hazard: A hazard with a moderate level of impact on critical business functions. Response should occur as soon as possible.

• Level3H - Level 3 Hazard: A hazard with a low degree of impact on critical business functions. Response may occur in 1 week.

• Level 1E - Level 1 Event: an event has occurred that has a high impact on critical business functions. The relevant procedures should be activated immediately.

• Level2E - Level 2 Event: an event has occurred that has a medium impact on critical business functions. The relevant procedures should be activated as soon as possible.

• Level3E - Level 3 Event: a low, low priority event.

11.Disaster Plan Update

The updating process if this Disaster Recovery Plan should always be properly structured and controlled. Any change to the plan should always be fully tested and the appropriate changes should be made to the training material.

Each section of this document is meant to be reviewed regularly and updated according to any new finding, any change in the company’s situation, technology or any other event that can cause this information to be considered obsolete.

12.Disaster Plan Testing

The procedures specified in the previous sections need to undergo regular and thorough testing to ensure their efficiency. In this section are descripted five ways to perform the tests.

**Paper test:** Memebers of the disaster recovery team go through the document annotating any issue or any change or improvement they would apport.

**Walk through test:** The DR team walk through the facility pinpointing any issue ar area of improvement.

**Simulation:** The DR team practice the disaster recovery procedures in real life to measure and assess their efectiveness.

**Parallel test:** Backup and recovery secondary systems are tested working simoultaneously with the primary system to control if they can perform the business transactions.

**Cutover test:** Backup and recovery secondary systems are tested by taking over the full workload of the primary systems. The primary systems are disconnected during the test.