Trendie

BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY AND PROCEDURES

Purpose

The purpose of this Business Continuity and Disaster Recovery Policy is to establish a comprehensive framework for ensuring the resilience of Trendie in the event of a disruption, whether due to natural disasters, technological failures, or other unforeseen events. This policy outlines the procedures for maintaining essential business functions and recovering from incidents to minimise operational, financial, and reputational impacts.

Scope

This policy applies to all departments, employees, and operations of Trendie, including third-party service providers and contractors. It covers the planning, implementation, and management of business continuity and disaster recovery activities, ensuring that critical business functions can continue or be restored promptly.

Objectives

- To ensure the safety and well-being of employees, clients, and stakeholders during a disaster or disruptive event.
- To minimise the impact of disruptions on business operations and maintain continuity of critical services.
- To comply with relevant Australian legislation, regulations, and industry standards, including the Privacy Act 1988 (Cth), Work Health and Safety Act 2011 (Cth), and the Australian Cyber Security Centre (ACSC) guidelines.
- To safeguard Trendie's assets, including physical, financial, intellectual, and informational resources.
- To establish a structured approach for disaster recovery, including restoring data, IT systems, and operational capacity.

Trendie

Business Continuity Principles

- **Risk Assessment and Management:**
  - Identify potential risks and threats that could disrupt business operations.
  - Conduct regular risk assessments and update the Business Continuity Plan (BCP) accordingly.
  - Implement risk mitigation strategies to minimise the impact of identified threats.
- **Emergency Response:**
  - Develop an Emergency Response Plan (ERP) to ensure a swift and coordinated response to incidents.
  - Provide training to employees on emergency procedures, including evacuation, communication protocols, and safety measures.
  - Ensure the availability of emergency resources, such as first aid kits, emergency contact lists, and backup communication systems.
- **Business Impact Analysis (BIA):**
  - Conduct a BIA to identify critical business functions, processes, and resources.
  - Determine the impact of potential disruptions on these functions and establish recovery priorities.
  - Define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for each critical function.
- **Continuity Planning:**
  - Develop and maintain a Business Continuity Plan (BCP) that outlines procedures for maintaining or restoring critical business functions.
  - Identify key personnel, roles, and responsibilities for implementing the BCP.
  - Establish communication protocols to ensure timely and accurate information is disseminated during a disruption.

- **Disaster Recovery Planning:**
    - Develop a Disaster Recovery Plan (DRP) that focuses on restoring IT systems, data, and infrastructure.
    - Ensure regular backups of critical data and systems are conducted and stored securely.
    - Test disaster recovery procedures regularly to validate their effectiveness and ensure readiness.
- **Compliance and Legal Considerations:**
    - Ensure compliance with Australian legislative and regulatory requirements, including data protection and privacy laws.
    - Maintain records of compliance activities, such as training, testing, and plan reviews, for audit and reporting purposes.

Responsibilities

- **Employees:**

  All employees are responsible for familiarising themselves with this policy and the associated procedures. They must participate in training and drills and follow instructions during an incident. Employees should also report any potential risks or incidents to their manager or the designated Business Continuity Officer.

- **Managers:**

  Managers are responsible for ensuring their teams understand and comply with the business continuity and disaster recovery procedures. They must support the development and maintenance of departmental continuity plans and ensure that employees are adequately trained.

- **Business Continuity Officer:**

  The Business Continuity Officer is responsible for overseeing the implementation of this policy. This includes coordinating risk assessments, business impact analyses, and the development of the BCP and DRP. They also manage training, testing, and review activities and ensure compliance with relevant legislation and standards.

- **IT Department:**

  The IT department is responsible for implementing and maintaining technical components of the disaster recovery plan, including data backups, system redundancy, and cybersecurity measures. They must ensure that IT systems are regularly tested and that recovery procedures are up to date.

Procedures

- **Risk Assessment and Business Impact Analysis:**
  - Conduct annual risk assessments to identify potential threats to business operations.
  - Perform a Business Impact Analysis (BIA) to determine the effects of disruptions on critical functions.
  - Update the risk register and BCP based on the findings.
- **Plan Development and Maintenance:**
  - Develop a comprehensive Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) tailored to the organisation's needs.
  - Review and update the BCP and DRP annually or after significant changes to business operations.
  - Document all changes and communicate them to relevant stakeholders.
- **Training and Awareness:**
  - Provide business continuity and disaster recovery training to all employees at least annually.
  - Conduct regular drills and exercises to test the effectiveness of the plans and identify areas for improvement.
  - Encourage employees to provide feedback on the drills and any aspects of the plans.

- **Incident Response and Recovery:**
  - Activate the Emergency Response Plan (ERP) immediately upon identification of an incident.
  - The Business Continuity Officer or designated Incident Commander will lead the response, coordinating with key personnel and stakeholders.
  - Implement the Business Continuity Plan (BCP) to maintain or restore critical functions within established RTOs and RPOs.
  - Implement the Disaster Recovery Plan (DRP) to restore IT systems and data as quickly as possible.
- **Communication Protocols:**
  - Establish a communication tree and ensure all employees have access to up-to-date contact information.
  - Use multiple communication channels, including email, SMS, and phone, to disseminate information during an incident.
  - Provide regular updates to employees, clients, and stakeholders on the status of the incident and recovery efforts.
- **Post-Incident Review and Continuous Improvement:**
  - Conduct a post-incident review to evaluate the effectiveness of the response and recovery efforts.
  - Identify lessons learned and incorporate improvements into the BCP and DRP.
  - Document the review findings and update the risk assessment and business impact analysis as necessary.

Compliance and Enforcement

Trendie is committed to ensuring compliance with this Business Continuity and Disaster Recovery Policy. Non-compliance with this policy may result in disciplinary action, including but not limited to, warnings, suspension, or termination of employment. Compliance will be monitored through regular audits, reviews, and testing of the BCP and DRP.

Trendie

Review and Updates

This policy will be reviewed annually or following a significant incident or change in business operations. Updates to this policy will be communicated to all employees and incorporated into the business continuity and disaster recovery training program.

Implementation

The Business Continuity Officer will oversee the implementation of this policy, ensuring all employees are trained and the necessary resources are allocated. The BCP and DRP will be accessible to all staff through the company intranet and the employee handbook.

By adhering to this policy, Trendie commits to safeguarding the continuity of its operations and the safety of its employees, clients, and stakeholders in the event of a disaster or disruption.