Business Continuity Plan Summary

CONTENTS

INTRODUCTION

PURPOSE

The purpose of the Business Continuity Plan is to ensure the continuity of Layershift's critical operations during and after a disruptive incident. This plan outlines the necessary steps to protect the company's data and resources, and to ensure that the company can maintain its operations and continue to provide services to its customers.

SCOPE

This Business Continuity Plan covers all of Layershift's critical operations, including Cloud VPS, PaaS, and ancillary services, and is designed to ensure that the company is able to continue providing services to its customers with minimal interruption.

CONFIDENTIALITY

Due to the sensitive nature of the Business Continuity Plan and the risks associated with disclosing it in full, this document is intended to summarise the contents for Layershift customers to have an understanding of some of the measures in place to protect their data and ensure service continuity without disclosing business sensitive information.

ROLES AND RESPONSIBILITIES

MANAGEMENT

The management team is responsible for ensuring the implementation, reviews, maintenance, testing and training of this plan.

OPERATIONS

The operations team is responsible for ensuring that the necessary technical resources, systems and processes are in place to support the plan.

OTHER TEAMS

The support team and other teams are responsible for following the procedures outlined in this plan and for taking the necessary steps to ensure that the company is able to continue operations.

RISK MANAGEMENT

RISK IDENTIFICATION

Layershift will identify and assess the risks associated with a major disruption, such as a power outage, network outage, data loss, security breach, cyber attack, fire, theft, natural disasters, infectious diseases and other emergencies.

RISK MITIGATION

Layershift will continuously develop and implement strategies to mitigate the risks associated with a major disruption.

Risk identified	Risk mitigation
Power outage	Redundant power sources are used in all locations providing customer services. Risk mitigation examples include: • UPS with redundancy (e.g. N+1, 2N, 2(N+N)) • Dual power feeds to racks • Continuous voltage regulation • Diesel generators with fuel re-supply contracts • Key vendor and employee contact list regularly updated and readily accessible
Network outage	Redundant network connectivity is used in all locations providing customer services. Risk mitigation examples include: • Upstream public network connectivity using redundant connections and diverse paths • Power redundancy for network infrastructure • Automatic failover, where possible • Key vendor and employee contact list regularly updated and readily accessible, including network engineer on-call 24x7
Data loss	The risk of data loss is mitigated in various ways: • Offsite backups (excluding Singapore) • Regular backup frequencies • Multiple restore points for backups available • Ability to restore backups to newly provisioned physical servers • Restricted access to backup servers • Redundant hard disk arrays (RAID) for all customer services • In-stock spare parts or hot/cold spare servers • Exclusive use of enterprise-grade SSDs and hard disk drives for live customer services • Key vendor and employee contact list regularly updated and readily accessible

Risk identified	Risk mitigation
Security breach / cyber attack	A comprehensive security policy is followed by all employees to mitigate risk of a security breach. Risk mitigation examples include: • Multi-factor authentication for all employee access to customer services • Regular monitoring of vendor mailing lists and other sources for security updates or risks • Prompt installation of high priority security updates • Non-stop kernel updates to patch security risks • Security first procedures and staff training • Network monitoring • Server logs enabled by default • Superuser access restricted for managed customer servers • Key vendor and employee contact list regularly updated and readily accessible
Fire	Fire suppression systems are operational 24x7 in all locations providing customer services. Risk mitigation examples include: • Proactive fire detection (e.g. VESDA) and suppression (e.g. FM200 / Argonite) • 24x7 temperature monitoring • 24x7 critical infrastructure monitoring • Priority response from emergency services • Ability to access hot/cold spare servers as required • Key vendor and employee contact list regularly updated and readily accessible
Theft	Secure facilities are used in all locations providing customer services. Risk mitigation examples include: • 24x7 on-site security or 24x7 remote monitoring • Secure datacentre facility • Controlled 24x7 datacentre access, including multi-factor identification • Restricted access to racks • Lockable industry-standard racks • Ability to access hot/cold spare servers as required • Key vendor and employee contact list regularly updated and readily accessible
Natural disasters	Facilities providing customer services operate taking into consideration the risks of natural disasters, which vary depending on their location. Risk mitigation examples include: • Facilities purpose-built or re-purposed considering natural disaster risks • Redundant power sources including generator backup • Regular testing of power redundancy including generator checks • Multiple geographical locations allow customer data to be moved or replicated upon request

Risk identified	Risk mitigation
Infectious diseases	A distributed team is in place to minimise the impact to customer services as a result of infectious diseases impacting Layershift's team. Risk mitigation examples include: • Employees encouraged to work from home, when possible • Geographically distributed team • Remote access to all systems • Physical access to all infrastructure can be securely managed for both internal staff and external contractors

INCIDENT RESPONSE

INCIDENT MANAGEMENT

In the event of a disruptive incident, the management team should be notified immediately. The operations team should be responsible for investigating the incident and determining the extent of the damage. The management team should then assess the situation and determine the necessary actions to take to ensure the continuity of operations. This should include the implementation of alternative systems and resources as necessary, and implementing the necessary technical measures to protect data and resources.

Other employees are allocated to different roles depending on the nature of the event, including customer communication, following recovery procedures, and supporting the operations team.

CONTINGENCY PLANNING

To minimise recovery time, a recovery time objective and recovery strategy is in place depending on the nature of the disruptive event.

Backup and recovery plan

Layershift will continuously develop and implement a comprehensive backup and recovery plan that outlines the steps that must be taken to ensure that the company is able to continue operation during and after a disruptive event.

Crisis management plan

Layershift will continuously develop and implement a crisis management plan that outlines the steps that must be taken to ensure the safety of all personnel during a disruption and to minimise the impact of the disruption on the company's operations.

Communication plan

Layershift will continuously develop and implement a communication plan that outlines how the company will communicate with employees, customers, vendors, and other stakeholders during a disruptive event.

Testing and evaluation

Layershift will regularly test and evaluate the results of the Business Continuity Plan a minimum of once per year to ensure that it remains effective in responding to disruptive events.

CONCLUSION

Layershift's Business Continuity Plan is designed to ensure that the company is able to continue providing services to its customers with minimal interruption in the event of a disruptive event. By implementing this Business Continuity Plan, Layershift can ensure the highest chance of successfully delivering the services customers need at all times.