STANDSS (SOUTH PACIFIC) PTE LTD

CYBER SECURITY INCIDENT RESPONSE PLAN

Version:	1.0.4
Date Issued:	13th July 2026
Date for Review:	01/07/2027

Contents

Contents 2
Goals for Cyber Incident Response 3
Purpose and scope 3
Incident Response Team (IRT) 3
Incident Response Life Cycle Process 4
Incident Occurrence & Awareness 5
Incident Response Process Detail 5
Communication Methods 6
Information Recording 7
Incident Response Exercises 7
Summary 7
Appendix A – Cyber Incident Response Team (IRT) 8
Appendix B - Incident Categorization 9
Appendix C – Incident Impact Definitions 10
Appendix-D IRT Incident Severity & Response Classification Matrix 11
Appendix-E IRT Incident Record Form 12
Appendix F- External Communications and Notification Plan 13
Updates 16
    Summary of Tabletop Exercise - Phishing Attacks on Standss Email 16
    Summary of Tabletop Exercise - Phishing Attacks on Standss Email 17
    Summary of Tabletop Exercise – Microsoft 365 Account Compromise Incident 18
Document Version History 20

Goals for Cyber Incident Response

When a cyber security incident occurs, timely and thorough action to manage the impact of the incident is critical to an effective response process. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Specifically, the response goals for Standss (South Pacific) PTE Ltd. are:

1. **Preserve and Protect Confidentiality, Integrity, and Availability**: Ensure the confidentiality of constituent and employee information and maintain the integrity and availability of Standss (South Pacific) PTE Ltd.'s systems, networks, and related data.

2. **Facilitate Business Process Recovery**: Assist Standss (South Pacific) PTE Ltd. personnel in recovering their business processes following a computer or network security incident or other types of data breaches to minimize disruption to operations.

3. **Implement a Consistent Response Strategy**: Provide a consistent response strategy to address system and network threats that jeopardize Standss (South Pacific) PTE Ltd.'s data and systems, ensuring a unified approach to incident handling.

4. **Develop and Activate Communication Plan**: Develop and activate a comprehensive communication plan that includes initial reporting of the incident and ongoing communications as necessary to keep stakeholders informed and minimize uncertainty.

5. **Address Legal Issues**: Address cyber-related legal issues promptly and effectively, ensuring compliance with relevant laws, regulations, and contractual obligations to mitigate legal and financial risks.

6. **Coordinate with External Teams and Law Enforcement**: Coordinate efforts with external Computer Incident Response Teams (CIRTs) and law enforcement agencies to leverage additional expertise and resources in responding to cybersecurity incidents and facilitate investigations when necessary.

7. **Minimize Reputational Risk**: Minimize Standss (South Pacific) PTE Ltd.'s reputational risk by responding transparently and effectively to cybersecurity incidents, maintaining customer trust, and safeguarding the company's brand reputation.

Purpose and scope

This publication provides practical guidelines on responding to cyber security and data breach incidents in a consistent and effective manner. The plan establishes a team of first responders to an incident with defined roles, responsibilities, and means of communication. While this plan is primarily oriented around cyber-related incidents and breaches, it can also be utilized for data breaches that are not related to computer systems.

Incident Response Team (IRT)

A team made up of company staff, advisors, and service providers will coordinate incident responses and is known as the Incident Response Team (IRT). The IRT includes individuals listed in Appendix A with assigned roles and responsibilities. Primary members are first responders or informed members for incidents requiring IRT involvement, based on severity.

The entire IRT is informed and involved in severe incidents. Members may take on additional roles as needed. Contact information, including email addresses and telephone numbers, is circulated among the team. The IRT may enlist additional staff or consultants, known as Subject Matter Experts (SMEs), for incident analysis, remediation, and recovery. The Information Technology (IT) function is crucial for technical aspects of incident detection and response and serves as an SME. An Incident Response Manager (IRM) is designated within the IRT to oversee organizational and coordination roles during activated incident responses.

Incident Response Life Cycle Process

Cyber incident response management is an on-going process with a cyclical pattern. The specific incident response process elements that comprise the Cyber Incident Response Plan include:

1. **Preparation:** The on-going process of maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, applications, and data handling processes are sufficiently secure, and employee awareness training is in place. Practice exercises (aka Table-top Exercises) for the IRT are conducted periodically, where various incident scenarios are presented to the Team in a practice session.

2. **Identification:** The process of confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents.

3. **Notification:** Alerting IRT members to the occurrence of an incident and communicating throughout the incident.

4. **Containment:** Minimizing financial and/or reputational loss, theft of information, or service disruption. Initial communication with constituents and news media, as required.

5. **Eradication:** Eliminating the threat.

6. **Recovery:** Restoring computing services to a normal state of operation and the resumption of business activities quickly and securely. Provide reputational repair measures and news media updates, if needed. Provide credit monitoring services to affected constituents, or other remediation measures, as appropriate.

7. **Post-incident Activities:** Assessing the overall response effectiveness and identifying opportunities for improvement through ‘lessons learned’ or mitigation of exploited weaknesses. Incorporation of incident’s learnings into the cyber fortification efforts and the response plan, as appropriate.

   These process elements are depicted in Figure 1, showing the closed loop nature of the process, in that the learnings from any prior incidents are used to improve the prevention and response process of potential future incidents.



Figure 1: Incident Response Life Cycle

Incident Occurrence & Awareness

The way an incident becomes know will have an impact on the response process and its urgency. Examples by which Standss becomes aware of an incident include, but are not limited to the following:

1. Standss (South Pacific) PTE Ltd discovers through its internal monitoring that a cyber incident or data breach has occurred.
2. Standss (South Pacific) PTE Ltd is notified by one of its technology providers of an incident or becomes aware of the same.
3. Standss (South Pacific) PTE Ltd is made aware of a breach through a constituent or a third-party informant.
4. Standss (South Pacific) PTE Ltd and the public are made aware of the incident through the news media.

Incident Response Process Detail

The response process, at a detail level, for an incident includes 5 of the 6 life cycle phases, as it excludes the Preparation phase. The detailed steps and general timing of an incident response are outlined below. The IT function is specifically called out as an involved party, separate from other SME's.

Process Phase & Approximate Timing	Process Detail Steps	Involved Parties
Identification **(Hours)**	1. Identify and confirm that the suspected or reported incident has happened and whether malicious activity is still underway. 2. Determine the type, impact, and severity of the incident by referring to **Appendices B, C, and D**. 3. Take basic and prudent containment steps.	IT and any monitoring service provider
Notification **(Hours – 1 Day)**	4. Inform or activate the IRT, based on the severity of the incident, as outlined in Appendix D, and provide the type, impact, and details of the incident to the extent that they are known. 5. Determine the need for Subject Matter Experts (SME) to be involved in the Containment, Eradication, and Recovery processes.	IT & IRT
Containment **(Hours-2 Days)**	6. Take immediate steps to curtail any on-going malicious activity or prevent repetition of past malicious activity. 7. Re-direct public facing websites, if needed. Provide initial public relations and legal responses as required.	IRT, IT, SME's
Eradication **(Days -Weeks)**	8. Provide full technical resolution of threat and related malicious activity. 9. Address public relations, notification, and legal issues.	IT, IRT, SME's
Recovery **(Weeks -Months)**	10. Recover any business process disruptions and re-gain normal operations. 11. Address longer term public relations or legal issues, if required, and apply any constituent remedies.	SME's, IRT
Post-incident **(Months)**	12. Formalize documentation of incident and summarize learnings. 13. Apply learnings to future preparedness.	IRT

Communication Methods

Company communication resources (email, phone system, etc.) may be compromised during a severe incident. Primary and alternate methods of communication using external infrastructure will be established and noted on the IRT member contact list to provide specific methods of communication during an incident.

The IRT and any other individuals involved in incident resolution will be directed as to which communication method will be used during the incident.

External communications with customers, service providers, regulators, business partners, insurers, and other relevant parties will be managed in accordance with **Appendix F – External Communications and Notification Plan**. The plan defines communication responsibilities, notification requirements, approval processes, communication content, and documentation requirements during a security incident.

Information Recording

Information recording is very important during an incident, not only for effective containment and eradication efforts, but also for post-incident lessons learned, as well as any legal action that may ensue against the perpetrators. Each member of the IRT shall be responsible for recording information and chronological references about their actions and findings during an incident, using the IRT Incident Record Form in Appendix E.

Incident Response Exercises

The IRT should conduct 'table-top' exercises to practice the response process on a periodic basis, but at least annually, so all members of the IRT are familiar with the activities that would occur during an actual incident and their related responsibilities. The exercises may provide the opportunity for enhancing the coordination and communication among team members.

Summary

No perfect script can be written for the detailed activity encountered and decisions that will need to be made during an incident, as each incident will have its own uniqueness. This plan shall serve as a framework for managing cyber security and data breach incidents, allowing the details of confirmation, containment, eradication, and communication to be tailored to fit the specific situation.

Appendix A – Cyber Incident Response Team (IRT)

Name	Role	Contact Information
Sanjay Singh	• Maintain proactive cybersecurity policies and procedures • Discover and/or verify cyber incidents • Notify IRT members of incidents and provide updated information • Coordinate computer forensic and technical remediation activities • Apply corrective actions to technology infrastructure	Phone: +679 9993421 Email: sanjays@standss.com
Deepak Chand (IRM)	• Coordinate communications and activities of the IRT when it is activated	Phone: +679 9369018 Email: chandd@standss.com
Pretika Goundar	• Financial impact and financial data exposure	Phone: +679 9968531 Email: goundarp@standss.com
Unaisi Ranasu	• Communication to employees • Employee data exposure issues	Phone: +679 9570888 Email: ranasuu@standss.com
Avishek Nand	• Detection • Mitigation • Technical Forensics	Phone: +679 7145349 Email: nanda@standss.com

Appendix B - Incident Categorization

COMMON CATEGORIES OF CYBER INCIDENTS

Incident Type	Type Description
Unauthorized Access	When an individual or entity gains logical or physical access without permission to a company network, system, application, data, or other resource.
Denial of Service (DoS, DDoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources.
Phishing	An attack that involves sending fraudulent emails or messages that appear to be from reputable sources, with the intention of tricking recipients into revealing sensitive information such as usernames, passwords, or financial details.
Ransomware	Malicious software designed to deny access to a computer system or data until a ransom is paid. Ransomware typically encrypts files or locks the system, rendering it unusable until the ransom is paid, often in cryptocurrency.
Malicious Code	Successful installation of malicious software (e.g., a virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
Improper or Inappropriate Usage	When a person violates acceptable computing policies, including unauthorized access or data theft.
Suspected PII Breach	An incident where it is suspected that Personally Identifiable Information (PII) has been accessed.
Suspected loss of Sensitive Information	An incident that involves a suspected loss of sensitive information (not PII) that occurred because of Unauthorized Access, Malicious Code, or Improper (or Inappropriate) use, where the cause or extent is not known.

Appendix C – Incident Impact Definitions

Security Objective	General Description	Potential Impact Examples		
		Low	Medium	High
Confidentiality: *Preserving restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*	The unauthorized disclosure of information could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Limited to a single or several Users or computers in an isolated fashion, with easy remediation	Involving or affecting a group of Users, resulting in access to proprietary information. Limited or no external exposure.	A severe breach of proprietary information with external exposure.
Integrity: *Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.*	The unauthorized modification or destruction of information could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Inadvertent or non-malicious alteration or deletion of company data that is easily remediated.	An on-going improper data alteration act (or series of acts) of malicious or negligent nature that will be having a moderate business impact.	A massive alteration or destruction of company data of a malicious or obstructive nature.
Availability: *Ensuring timely and reliable access to and use of information systems.*	The disruption of access to or use of information or an information system could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Isolated outage or inaccessibility affecting a limited number of Users for a short amount of time (< 2 hours)	A widespread outage or inaccessibility of a primary business system lasting more than 2 hours, but less than a day	Severe outage or inaccessibility of the company business systems lasting a day or more.

Appendix-D IRT Incident Severity & Response Classification Matrix

Severity Level (5=Most Severe)	Typical Incident Characteristics	Example of Impact	Incident Response	Activate IRT?
5	DDoS attack against hosted Servers. Active attacks against network infrastructure. Access to internal company data by nefarious parties.	An enterprise-wide attack involving multiple departments that prevents access to systems and disrupts business operations. Access to or theft of proprietary data.	IRT and the IRM direct response. Remediation coordinated by IT, Forensics, and SME's. Possible Legal Counsel, Law Enforcement involvement	Full Team Active
4	Affects data or services for a group of individuals and threatens sensitive data, or involves accounts with elevated privileges with potential threat to sensitive data	Compromised business application. Improper or unauthorized access to data.	Response coordinated by IRM, IT, and SME's; IRT advised. Legal Counsel specifically notified if there is a PII breach.	Full Team Informed and Advised
3	Affects data or services of a single individual, but involves significant amounts of sensitive data, may include PII.	Employee computer or account with sensitive data access compromised, physical theft of device, unprotected media, or hard copy data.	Response coordinated by IT or IRM, with information sent to the IRT members. Legal Counsel notified if a PII breach	Primary Team Informed
2	Affects data or services of a group of individuals with no sensitive data involved.	Compromise of an account or device with shared folder access.	Response coordinated by IT. IRM advised and IRT informed. IT documentation process used to record findings.	Primary Team Informed
1	Affects data or services of a single individual with no sensitive data beyond them; focus is on correction and future prevention	Compromised computer with no sensitive data etc.	Documentation of issue and findings. Response/remediation coordinated by IT, IRM advised of incident.	No
0	Occurrences of very minor or undetermined focus, origin and/or effect for which there is no practical follow-up	Impaired computer requiring review of system access logs, AV scans, or other repairs.	Documentation through normal IT support processes to record actions and resolution. Reset passwords as needed.	No

Appendix-E IRT Incident Record Form

Incident: _____

Discovery Date: _____

Recorded By: _____ Page _____ of _____ Pages

Recorded Information and Events

Date/Time	Detail

Appendix F- External Communications and Notification Plan

1. Purpose

The purpose of this External Communications and Notification Plan is to establish a consistent and controlled approach for managing external communications during cybersecurity incidents, data breaches, or significant service disruptions affecting Standss (South Pacific) PTE Ltd.

Effective communication is essential during an incident to ensure that relevant stakeholders receive accurate and timely information while maintaining confidentiality, meeting regulatory obligations, protecting customer trust, and supporting effective incident management.

This plan forms part of the Standss Cyber Incident Response Plan and should be followed whenever an incident requires communication with parties outside the organisation.

2. Communication Governance

All external communications relating to cybersecurity incidents must be coordinated through the Incident Response Team (IRT). The Incident Response Manager (IRM) is responsible for coordinating communication activities and ensuring that notifications are made to appropriate parties based on the severity, impact, and nature of the incident.

Technical information relating to the incident will be provided by the IT function and relevant Subject Matter Experts (SMEs). Management is responsible for approving significant external communications, particularly communications involving customers, regulators, legal matters, or reputational impact.

Only authorised representatives of Standss may communicate externally regarding confirmed security incidents.

3. External Notification Assessment

Following identification and classification of a security incident, the Incident Response Team will assess whether external notification is required. The assessment will consider the type of incident, affected systems, data involved, customer impact, contractual requirements, and applicable regulatory obligations.

The following table defines the external parties that may require notification.

External Party	Notification Criteria	Responsibility
Customers	Notification may be required where customer data, customer services, or customer operations are affected.	Incident Response Manager / Management
Microsoft Azure and Microsoft 365	Notification may be required where cloud infrastructure, identity services, or Microsoft-managed services are involved.	IT Team
Technology Service Providers	Notification may be required where third-party applications, integrations, or supporting services are affected.	IT Team
Business Partners	Notification may be required where shared services, contractual obligations, or integrations are impacted.	Management
Regulatory Authorities	Notification may be required where legal or regulatory obligations require reporting of an incident.	Management / Legal Advisor

Data Protection Authorities	Notification may be required where a personal data breach meets applicable reporting requirements.	Management / Privacy Representative
Cyber Insurance Provider	Notification may be required where the incident falls within cyber insurance reporting obligations.	Management
Law Enforcement	Notification may be required where criminal activity, fraud, unauthorised access, or legal investigation is involved.	Management

4. Notification Timeframes
Standss will assess and communicate security incidents according to the severity and impact of the event. Internal escalation to relevant personnel will occur as soon as an incident requiring response is confirmed.

External notifications will be performed within applicable contractual, legal, and regulatory timeframes. Where customer notification is required, communication will occur as soon as sufficient information is available to provide accurate and meaningful information.

For incidents involving personal information, Standss will assess notification requirements under applicable privacy legislation. Where GDPR obligations apply and a reportable personal data breach has occurred, notification to the relevant supervisory authority will be completed within 72 hours of becoming aware of the breach.

5. External Communication Process
When an incident requires external communication, the Incident Response Manager will coordinate the notification process.

The process will include reviewing the incident details, confirming affected systems or information, identifying required recipients, preparing communication content, obtaining required approval, issuing notifications, and recording all communication activities.

The following information should be included in external incident communications where applicable.

Information Category	Description
Incident Summary	Description of the incident and how it was identified.
Incident Timing	Date and time the incident occurred or was detected.
Impact Assessment	Systems, services, customers, or information affected.
Response Actions	Containment, investigation, and remediation activities completed or underway.
Customer Actions	Recommended actions for affected customers or stakeholders.
Contact Information	Appropriate contact details for follow-up communication.
Recovery Status	Updates regarding restoration of services and ongoing improvements.

6. Communication Methods
External communications may be conducted using approved communication channels, including official company email, customer support channels, direct customer communication, vendor security portals, telephone communication, or regulatory reporting platforms.

Where normal communication channels are unavailable due to the incident, the Incident Response Team will use alternative communication methods documented within the IRT contact list.

7. Communication Records and Tracking
All external communications relating to cybersecurity incidents must be recorded as part of the incident management record.

The Incident Response Team will maintain records of communications, including the date and time of communication, recipient details, communication method, responsible person, information provided, decisions made, and any required follow-up actions.

These records will be retained with the incident documentation to support investigation activities, regulatory requirements, audit reviews, and post-incident improvement activities.

8. Post-Incident Communication Review
Following completion of incident recovery activities, the Incident Response Team will review the effectiveness of external communications undertaken during the incident.

The review will consider communication timeliness, stakeholder feedback, notification decisions, and opportunities to improve future incident response activities. Lessons learned will be incorporated into updates to the Cyber Incident Response Plan where required.

Updates

Summary of Tabletop Exercise - Phishing Attacks on Standss Email

The tabletop exercise conducted on 21/02/2024 focused on phishing incidents targeting Standss emails, the organization evaluated its readiness and response procedures. The exercise aimed to assess various aspects of incident response, including initial detection, impact assessment, containment, communication, and lessons learned.

Key Findings:

- **Initial Detection and Response:** Automated email filtering systems were effective in flagging suspicious emails, and the IT security team promptly initiated investigations upon receiving reports. However, there were areas identified for improvement in terms of analyzing email headers and verifying sender authenticity.

- **Impact Assessment:** Tools such as intrusion detection systems and digital forensics techniques were utilized to assess the extent of the breach and prioritize critical assets for protection. Enhancements were recommended in terms of analyzing logs and identifying potential data exfiltration.

- **Containment and Mitigation:** Immediate actions were taken to disable compromised accounts, block malicious domains, and isolate affected systems. Strategies were proposed to further enhance containment measures and prevent future phishing attempts through employee awareness training and multi-factor authentication.

- **Communication and Coordination:** Communication channels among incident response team members and stakeholders were effectively utilized to disseminate information and updates. Recommendations were made to streamline communication processes and improve external stakeholder engagement during incidents.

- **Lessons Learned and Recommendations:** Key challenges included delays in detection and response, gaps in employee awareness, and coordination issues. Lessons learned emphasized the importance of continuous monitoring, enhanced training, and refined incident response procedures. Recommendations focused on implementing advanced email filtering solutions, conducting regular phishing simulations, and fostering a culture of cybersecurity awareness.

Conclusion:
The tabletop exercise provided valuable insights into the organization's strengths and areas for improvement in responding to phishing incidents targeting Standss emails. By addressing the identified challenges and implementing the recommended enhancements, the organization aims to bolster its resilience against phishing threats and strengthen its overall cybersecurity posture.

This summary serves to highlight the key outcomes and action points derived from the exercise, guiding future updates and improvements to the Incident Response Plan.

Summary of Tabletop Exercise - Phishing Attacks on Standss Email

The tabletop exercise conducted on **03/06/2025** focused on phishing incidents targeting Standss emails. The organization evaluated its readiness and response procedures through a simulated phishing scenario involving a deceptive email impersonating a senior executive. The exercise aimed to assess various aspects of incident response, including initial detection, impact assessment, containment, communication, and lessons learned.

Key Findings:

- **Initial Detection and Response:**
  The phishing email was identified due to suspicious content and impersonation tactics. While automated email filters flagged the message, manual reporting by staff was key to timely detection. The exercise highlighted the need for improved analysis of email metadata and more robust sender verification practices.

- **Impact Assessment:**
  No data loss occurred, but the scenario reinforced the importance of promptly evaluating potential access or compromise. Current systems were effective in detecting unusual activity, but enhancements were recommended in reviewing email logs and ensuring rapid identification of targeted individuals or departments.

- **Containment and Mitigation:**
  The response included blocking the sender, isolating the affected message, and reinforcing password protocols. Preventative measures such as enhanced filtering rules and employee training were recommended. Multi-factor authentication and phishing-resistant policies were identified as critical for reducing risk.

- **Communication and Coordination:**
  Internal communication was timely and effective. Team members used designated channels to share updates and escalate concerns. However, the need for a clearer process to notify external stakeholders, such as partners or clients, was noted as an area for improvement.

- **Lessons Learned and Recommendations:**
  Challenges included slight delays in escalation and inconsistent application of reporting procedures. The exercise emphasized the value of ongoing awareness training, regular phishing simulations, and more structured coordination among departments. Recommendations included integrating AI-based detection tools, refining escalation protocols, and fostering a proactive cybersecurity culture.

Conclusion:

The tabletop exercise provided valuable insights into the organization’s strengths and areas for improvement in addressing phishing incidents. By taking proactive steps to address the identified gaps and adopting the recommended measures, Standss aims to enhance its resilience to email-based threats and strengthen its overall cybersecurity framework.

This summary highlights the key outcomes and action points derived from the exercise and will inform future updates to the organization’s Incident Response Plan.

Summary of Tabletop Exercise – Microsoft 365 Account Compromise Incident

The tabletop exercise conducted on 22/06/2026 focused on a simulated Microsoft 365 account compromise resulting from a phishing attack. The exercise assessed Standss South Pacific's ability to detect, investigate, contain, and recover from a cloud-based security incident involving unauthorized access to a user account. Participants worked through a realistic scenario where an attacker gained access to a Microsoft 365 account, created malicious email forwarding rules, and sent fraudulent emails to internal staff and external customers.

The exercise was designed to evaluate the effectiveness of the organization's Incident Response Plan, communication processes, and technical controls for responding to identity-based cyber threats.

Key Findings:

- **Initial Detection and Response:**

The simulated compromise was identified through multiple indicators, including unusual login activity from a foreign location, suspicious outbound emails, and customer reports of fraudulent communications. Participants demonstrated an understanding of the escalation process and recognized the importance of promptly activating the Incident Response Plan. The exercise reinforced the need for continuous monitoring of authentication events and rapid investigation of suspicious account activity.

- **Impact Assessment:**

The team assessed the potential impact of unauthorized access to company email systems, including the exposure of sensitive information, fraudulent communications, and reputational damage. Participants reviewed how to determine the scope of affected users, identify accessed information, and evaluate potential customer impact. The exercise highlighted the importance of maintaining accurate audit logs and documenting incident timelines.

- **Containment and Mitigation:**

The response strategy included disabling the compromised account, revoking active sessions, resetting credentials, re-enrolling multi-factor authentication, and removing malicious mailbox forwarding rules. The team also discussed reviewing other user accounts for indicators of compromise and preserving evidence before remediation actions were taken. Existing controls were considered effective, although opportunities for strengthening monitoring and alerting capabilities were identified.

- **Communication and Coordination:**

Internal communication between technical teams, management, and incident response personnel was effective throughout the exercise. Participants followed established reporting channels and escalation procedures. The exercise also highlighted the importance of maintaining clear communication with customers and stakeholders in the event that fraudulent emails are distributed from compromised accounts.

- **Lessons Learned and Recommendations:**

The exercise identified several opportunities for improvement, including enhanced monitoring of Microsoft 365 sign-in activity, stronger Conditional Access policies, and improved alerting for mailbox forwarding rule creation. Additional phishing awareness training and periodic reviews of privileged account access were recommended. Participants

also suggested conducting regular cloud security tabletop exercises to maintain readiness and ensure familiarity with evolving threats.

Conclusion:

The tabletop exercise provided valuable insights into the organization's preparedness to respond to a Microsoft 365 account compromise. Participants demonstrated a strong understanding of incident response procedures and effectively worked through the identification, containment, recovery, and communication phases of the incident lifecycle.

By implementing the recommendations identified during the exercise, Standss South Pacific will further strengthen its identity security controls, improve incident response capabilities, and enhance its resilience against account compromise and phishing-related threats.

This summary highlights the key outcomes and action items resulting from the exercise and will support future improvements to the organization's Incident Response Plan and cybersecurity program.

Document Version History

Version Number	Date	Author	Significant changes on previous version
1.0.0	21/01/2024	Shiva Prakash	Initial compilation
1.0.0	23/01/2024	Akif Hussain	Review & Approval
1.0.1	22/01/2024	Avishek Nand	Update – From Tabletop exercise (21/02/24)
1.0.2	04/06/2025	Shiva Prakash	Update – From Tabletop exercise (03/06/25)
1.0.3	23/06/2026	Shiva Prakash	Update – From Tabletop exercise (22/06/26)
1.0.4	13/07/2026	Shiva Prakash	Added External Communications and Notification Plan