Incident Response Plan

1. Introduction

The Incident Response Plan (IRP) outlines the procedures and actions OurProperty.com.au will take to effectively manage and respond to data breaches and other security incidents involving Personal Data. This plan ensures that we are prepared to handle incidents promptly, mitigate risks, and comply with legal obligations.

2. Objectives

The primary objectives of the Incident Response Plan are to:

- Identify and assess security incidents involving Personal Data.
- Contain and mitigate the impact of the incident.
- Communicate effectively with stakeholders, including affected individuals and regulatory authorities.
- Recover from the incident and restore normal operations.
- Review and improve our security practices based on lessons learned.

3. Incident Definition

A security incident is defined as any event that compromises the confidentiality, integrity, or availability of Personal Data. Examples of incidents include:

- Unauthorised access to Personal Data.
- Data breaches or leaks.
- Malware infections or ransomware attacks.
- Loss or theft of data storage devices.
- System failures affecting data processing or storage.

4. Incident Reporting

4.1. Reporting Channels

- **Internal Reporting:** Employees, contractors, and affiliates must report any suspected or confirmed data security incidents immediately to the designated Incident Response Team (IRT) through the following channels:
    - Email: russell@our.property
    - Slack: General channel
    - Skype:
    - Phone: +61 414 334 198
- **External Reporting:** In cases where an incident involves external parties, such as customers or vendors, the IRT will coordinate communication with these parties.

4.2. Reporting Timeline

- All incidents must be reported as soon as they are identified. Delays in reporting can increase the risk of data loss or further compromise.

5. Incident Response Team (IRT)

5.1. Composition The Incident Response Team is composed of representatives from key departments, including:

- Data Protection Officer (DPO)
- IT Security Manager
- Legal Counsel
- Communications Manager
- IT Support Manager

5.2. Responsibilities

- **Data Protection Officer (DPO):** Oversees the incident response process, ensures compliance with legal requirements, and liaises with regulatory authorities.
- **IT Security Manager:** Manages technical aspects of incident investigation, containment, and remediation.
- **Legal Counsel:** Provides guidance on legal implications and regulatory requirements.
- **Communications Manager:** Handles internal and external communications, including notifications to affected individuals and stakeholders.
- **IT Support:** Assists with technical support and recovery efforts.

6. Incident Handling Procedures

6.1. Identification and Assessment

- Confirm whether the event is a security incident.
- Assess the severity and impact of the incident, including the type of Personal Data involved and the potential risks to affected individuals.

6.2. Containment

- Implement measures to contain the incident and prevent further data loss or compromise. This may include isolating affected systems, disabling compromised accounts, or stopping unauthorised activities.

6.3. Eradication

- Identify and remove the root cause of the incident, such as malware or vulnerabilities. Ensure that all traces of the incident are addressed and eliminated.

6.4. Recovery

- Restore affected systems and services to normal operation. Verify that systems are secure before resuming full functionality.

6.5. Notification

- Notify affected individuals, regulatory authorities, and other relevant stakeholders as required by law. Provide clear and accurate information about the incident, its impact, and the steps taken to address it.

6.6. Documentation

- Maintain detailed records of the incident, including the timeline of events, actions taken, and communications made. This documentation is essential for compliance and future reference.

7. Post-Incident Review

7.1. Analysis

- Conduct a thorough review of the incident to understand what happened, how it was handled, and what improvements can be made.

7.2. Reporting

- Prepare a post-incident report summarising the incident, response actions, and recommendations for improvements. Share the report with relevant stakeholders and use it to update the Incident Response Plan and security practices.

7.3. Training and Awareness

- Based on the lessons learned, update training programs and security awareness initiatives to prevent similar incidents in the future.

8. Plan Review and Updates

The Incident Response Plan will be reviewed and updated annually or as needed to reflect changes in our operations, technology, or regulatory requirements. The updated plan will be communicated to all relevant stakeholders.

9. Contact Information

For any questions or concerns regarding this Incident Response Plan, please contact the Incident Response Team at:

- Email: russell@our.property
- Phone: +61 414 334 198