Digipixel Pte Ltd Incident Response Plan

<Change Log> A record of all the change details, e.g. change log number, changes made, name of personnel making the change, date, etc.	
1. **Preparation** Preparation for an incident response is not just about preparing to handle an incident when it happens. It also entails the prevention of incidents by ensuring that systems, networks, and applications are sufficiently secure.	
Preparing to handle incidents	Identify key contact information: ☐ Designate an incident response handler within your organisation ☐ Designate a data breach management team within your organisation. The team should comprise specific individual(s) with expertise in handling data breaches, the data protection officer ("DPO"), and a senior management representative ☐ Appoint a third-party incident response provider ☐ Contacts for product/service vendor(s) ☐ Regulatory bodies ☐ Law enforcement agencies ☐ SingCERT ☐ Clients ☐ Personal Data Protection Commission (PDPC) (if an organisation collects, uses and/or discloses individuals' personal data) ☐ Others: _____
Recognising possible attack vectors	Organisations should generally be prepared to handle any incidents, including data breaches. They can first identify and understand the types of attacks that could affect the organisation (which may also result in a data breach), then develop action plans to deal with each type of attack. Common attack vectors or entry points that threat actors may use are : ☐ Malware ☐ Phishing ☐ Distributed denial of service ☐ Ransomware ☐ Data breach ☐ Data corruption

	Poorly designed web applications Misconfigured systems Internet downloads Poor cyber hygiene practices (e.g. use of weak or default passwords, use of outdated software, etc.) Human lapses Authorised third parties Others: _____ Possible activities that may result in a data breach include but are not limited to: Hacking, ransomware, distributed denial of service incidents or unauthorised access to databases containing personal data Unauthorised modification or deletion of personal data Theft of computer notebooks, data storage devices or paper records containing personal data Scams (e.g., phishing attacks) that trick organisations into releasing personal data of individuals Loss of computer notebooks, data storage devices, or paper records containing personal data Sending personal data to a wrong email or physical address, or disclosing personal data to a wrong recipient Unauthorised access or disclosure of personal data by employees Improper disposal of personal data (e.g. hard disk, storage media or paper documents containing personal data sold or discarded before data is properly deleted) Others: _____
Reviewing possible sources of precursors and indicators	☐ Security software (e.g. Intrusion Detection Systems [IDS], Security Information and Events Management System [SIEM], anti-virus software, third party monitoring services, etc.) ☐ Logs (e.g. operating system logs, service and application logs, network device logs, netflow logs, etc.) ☐ Publicly available information (e.g. SingCERT alerts, alerts from products/services vendors on vulnerabilities, etc.) ☐ People from your organisation ☐ Others: _____
Develop, communicate, and exercise the plans	Develop relevant plans: ☐ Prevention and detection plans ☐ Containment, eradication, and recovery plans ☐ Crisis management and communications plans ☐ Business continuity plans ☐ Data breach management plans

	Others: _____ Action plans developed to respond to common incidents should be accessible, and any updates should be communicated to relevant parties (e.g. employees, vendors, etc.): Communications with employees and key stakeholders User awareness and training Regular reviews and updates of plans (e.g. when systems are onboarded, to new hires, or at regular scheduled intervals) Walk-through/exercise the plans Others: _____
2. **Detection and Analysis** The detection and analysis of an incident is the first step to identifying an incident and understanding its impact and severity.	
Making an initial assessment and prioritising the next steps	☐ Correlate events against the baseline to determine if an incident has occurred ☐ Check incidents against known threats precursors and indicators ☐ Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch ☐ Prioritise the incident handling activities, including whether to activate crisis management, and crisis communications plans ☐ Others: _____ If a data breach has been discovered/is suspected to have occurred, the data breach management team will conduct an initial assessment to determine the severity of the data breach. The initial assessment should include the following considerations: ☐ Cause of the data breach and whether the breach is still ongoing ☐ Number of affected individuals ☐ Type(s) of personal data involved ☐ The affected systems, servers, databases, platforms, services, etc. ☐ Whether help is required to contain the breach ☐ The remediation action(s) that the organisation has taken or needs to take to reduce any harm to affected individuals resulting from the breach ☐ Others: _____
Gathering evidence	Evidence gathering may serve two purposes – incident resolution and legal proceedings. Some of the evidence that need to be documented include: ☐ Summary of the incident ☐ Incident indicators

	System events Actions taken during the incident Logs of affected systems Forensic copies of affected systems Others: _____
Knowing your stakeholders and/or fiduciary obligations	Notify relevant stakeholders and affected parties ☐ Board of Directors ☐ Regulators, law enforcement and other government agencies (SPF, CSA, SGX, PDPC etc.) ☐ Clients ☐ Media ☐ Others: _____ An organisation should act swiftly as soon as it is aware of a data breach, whether suspected or confirmed. ☐ Upon the discovery of a data breach (suspected or confirmed), staff are to report the breach to the Business Unit (BU) heads. ☐ BU heads are to inform the Data Protection Officer (DPO) regarding the potential data breach. ☐ DPO is to activate the data breach management team and update senior management on the potential data breach. ☐ Others: _____
3. **Containment, Eradication & Recovery** This is one of the most critical stages of incident response. The strategy for containment and recovery is based on the information and indicators of compromise gathered during the analysis phase. The threat needs to be thoroughly eradicated before normal operations can resume to minimise subsequent repeated disruptions.	
Developing a Containment Strategy	Containment strategies vary depending on the type of incident, and a strategy should be developed for different incident types to contain the incident/data breach and minimise damage. Some of the more common strategies are: ☐ Isolate all or parts of the compromised network by disconnecting all affected systems ☐ Re-route or filter network traffic ☐ Prevent further unauthorised access to the system. Disable or reset the passwords of compromised user accounts ☐ Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system ☐ Firewall filtering ☐ Close vulnerable ports and mail servers ☐ Block further unauthorised access to the system ☐ Stop the identified practices that led to the data breach

	Establish whether the lost data can be recovered and implement further action to minimise any harm caused (e.g. remotely disabling a lost notebook containing a personal data of individuals, recalling an email that has been accidentally sent or forwarded etc.) Others: _____
Eradicating the threat	After containing the incident, eradication may be necessary to eliminate all traces of the incident. This may include: ☐ Wiping out the malware ☐ Disabling breached user accounts ☐ Patching vulnerabilities that were exploited. This should be applied to all affected hosts within the organisation ☐ Others: _____
Assessing the data breach	If a data breach has occurred, upon the containment of the data breach, the data breach management team shall conduct an in-depth assessment of the data breach, the success of its containment action(s) taken, and the efficacy of any technological protection applied on the personal data involved in the data breach. The data breach management team shall consider the following in the assessment of the data breach: ☐ Context of the data breach ☐ Ease of identifying individuals from the compromised data ☐ Circumstances of the data breach Crucially, the organisation will also have to determine if it is required to notify the PDPC and/or affected individuals of the breach as required by the PDPA.
Reporting data breaches to PDPC	In the case of a data breach, the DPO shall notify relevant stakeholders and affected parties from the time the data breach management team has determined that the data breach is notifiable under the PDPA. ☐ Regulators, law enforcement and other government agencies, such as the PDPC, as soon as practicable, but in any case, no later than three (3) calendar days ☐Affected individuals as soon as practicable, at the same time or after notifying the PDPC ☐ Others:_____ **Note:** Organisations may refer to the PDPC's Guide on Managing and Notifying Data Breaches under the PDPA for more information.
Taking steps towards recovery	This may entail: ☐ Restoring systems from backups

	Rebuilding systems from scratch Changing passwords (both administrators and users) Tightening network perimeter security Confirming the integrity of business systems and controls Others: _____
Monitoring and maintaining vigilance	☐ Continue to monitor the network for any anomalous activity or signs of intrusion ☐ Depending on the incident, organisations may need to consider higher levels of system logging or network monitoring ☐ Others: _____
4. **Post-Incident Review** Organisations should proactively review their plans and response activities to identify and resolve deficiencies and strengthen their security posture.	
Conducting post-incident review	☐ Identify and resolve deficiencies in systems and processes that led to the incident ☐ Identify and resolve deficiencies in planning and execution of your incident response plan ☐ Assess if additional security measures are needed to strengthen the security posture of your organisation ☐ Communicate and build on lessons learnt ☐ Others: _____ If a data breach has occurred, the data breach management team shall review and learn from the data breach to improve on their personal data handling practices. The review may involve the following: ☐ A review including a root cause analysis of the data breach ☐ A prevention plan to prevent similar data breaches in future ☐ Audits to ensure prevention plan is implemented ☐ A review of existing policies, procedures, and changes to reflect the lessons learnt from the review ☐ Changes to employee section and training practices ☐ A review of data Intermediaries involved in the data breach ☐ Others: _____
<Sign Off> Mr. Tan Yong Li (Leon), Director, Digipixel Pte. Ltd., CAA 110924.	