DigiKnight Technologies, Inc.

Incident Response Plan

Version: v0.6

Updated: 12/12/2021

MS511 Group 2

Kendall Boone

Kyle Carver

Jake O'Connor

Cody Pritchett

Tamonica Russell

Change Log

Date - Version	Change Summary	Author
11/10/2021 - v0.1	Established document format.	O'Connor, Jake
11/12/2021 - v0.2	Populated introduction section. Populated roles and responsibilities section. Populated incident category section.	O'Connor, Jake
11/20/2021 - v0.3	Updated formatting.	O'Connor, Jake
11/22/2021 - v0.4	Filling risk assessment and critical functions.	O'Connor, Jake
12/11/2021 - v0.5	Added Incident Response Steps. Updated and normalized formatting.	O'Connor, Jake
12/12/2021 - v0.6	Updated Security Risk Assessment with team mitigation tactics.	O'Connor, Jake

Contents

1 Introduction

1.1 Purpose

The primary purpose of this plan is to limit the impact of an information security incident on DigiKnight Technologies, Inc. as well as its employees, customers, and business partners. Achieving this purpose requires quick action and a coordinated approach from all parties involved.

1.2 Scope

The scope of this plan is limited to only security incidents and breaches (as defined below), but covers those that affect all DigiKnight Technologies, Inc. properties, employees, contractors, customers, and third parties associated with the company.

1.3 Definitions

Incident

A security incident is any event which violates the information security policies and procedures as defined by DigiKnight Technologies, Inc..

Breach

A breach is any event which results in the unlawful and unauthorized acquisition of information that compromises the security, confidentiality, or integrity of personal data. Depending on the scope of a breach it may be necessary to notify affected individuals, companies, and contractors as well as regulatory authorities and governmental bodies.

Personal Data / Personally Identifiable Information

Personal data is one or more pieces of information which can uniquely identify an individual. The exact definition of this term varies by region and regulation, but examples of personally identifiable information include SSN, driver’s license, credit card number and security code, or IP address.

Anonymization

Anonymization is the process by which data is stripped of personal information to the point where it can no longer be considered personally identifiable information.

Pseudonymization

Pseudonymization is the process by which data is mutated such that it no longer contains any personally identifiable information on its own but can be attributed to an individual through a separately contained and secured data source.

2 Roles and Responsibilities

2.1 Team Definitions

Role	Responsibility	Trigger
Incident Response Team	1. Lead investigations into information security incidents. 2. Take actions and activate team members in order to contain and control systems affected by incidents. 3. Maintain detailed history of security incidents and their resolution.	Engaged in all incidents.
IT Team	1. Provide support and expertise to the incident response team. 2. Take actions in order to contain and control systems affected by incidents. 3. Take appropriate steps to preserve information helpful to an incident investigation.	The IT Team is activated when an information security incident involves a system they support.
Communication Team	1. Manage internal incident communications with employees and stakeholders. 2. Manage external incident communications with media, regulators, and outside stakeholders.	The Communication Team is activated when an incident requires large-scale internal or external communication.
Physical Security Team	1. Provide insight and investigation into physical security components of incidents. 2. Provide security and support during incident investigations.	The Physical Security Team is activated when an incident affects the safety of personnel, the security of company property, or requires the preservation of physical evidence.

2.2 Incident Response Team

Role	Name	Contact Number
Team Leader	Alicia McKellips	415-555-8352 x190
Sponsor	Carlton Smith	415-555-7841
Team Member	Robert Wildhorn	415-555-8352 x194
Team Member	Joseph Webber	415-555-8352 x193

3 Security Risk Assessment

Risk Description	Mitigation/Response	Risk Category	Risk Assessment
Website Outage	Redundant web servers, site backups, automated outage notifications. Contact vendor(s) to provide assistance.	CAT 8	Low
Cybersecurity Breach	Staff security training, social engineering training, clear policies and procedures. Daily full backups (local), paired with weekly cloud backups to prevent data loss.	CAT 1	High
Insider Threat	Internal investigation team, anonymous reporting procedures. Conduct unannounced drills every 6-8 weeks on random rotation.	CAT 9	Medium
Database Vulnerability	Firewalls, proxy servers, software updates. Continuous differential backups.	CAT 7	High
Network Outage	Backup hardware in place, ISP emergency contact procedures. Daily full backups (local), paired with weekly cloud backups to prevent data loss.	CAT 8	High
PII Breach	Staff security training, clear policies and procedures, government/regulator notification process, public notification process. Daily full backups (local), paired with weekly cloud backups to prevent data loss.	CAT 2	Medium
Vulnerable Legacy Technology	Deprecated technology update schedule, firmware/patch update schedule. Contact vendor(s) to provide assistance.	CAT 7	Medium

4 Critical IT Functions

#	Function	Criticality	Max Downtime	Required Resources
1	Company Website	Medium	1-2 days	Internet Access, Web Server
2	Computer Backups	Medium	< 1 day	Local Servers, Offsite Servers, Backup Software, Internet Access
3	Customer Records	High	< 3 hrs	Customer Database, Customer Records Software
4	Employee E-Mail	High	< 3 hrs	Internet Access, Email Server
5	Inventory Records	High	< 3 hrs	Local Servers, Inventory Software
6				
7				
8				
9				

5 Incident Response Steps

#	Goal	Description
1	**Identify**	Automated security scans perform significant oversight on our digital assets, but individual employees should be on the look out for potential cybersecurity incidents and threats. Individuals who notice unexpected or undesired system behavior, or feel there is a potential cybersecurity threat should contact a member of the Incident Response Team as soon as possible.
2	**Categorize**	Once the Incident Response Team is alerted of a potential cybersecurity threat, they shall use the information provided by the reporter to categorize the incident based on its severity. Formalized severity categories can be found in Appendix A.
3	**Notify**	Once the Incident Response Team has categorized the incident, they shall notify stakeholders, emergency services, and vendors as appropriate for the situation.
4	**Correlate**	Once the Incident Response Team has notified the necessary individuals, they shall use the threat category and characteristics of the threat to identify an individual response plan. If no existing plan covers the exact threat, the Incident Response Team shall use their judgement to identify a suitable stand-in.
5	**Implement**	Once the Incident Response Team has identified an appropriate individual response plan, they, and any additional stakeholders brought in, will follow the steps of the plan to mitigate the effects of a cybersecurity incident and restore critical functionality.
6	**Audit**	Once the Incident Response Team has restored critical functionality and contained the threat, they shall perform an audit of the process. All incident response actions must be documented as they are taken so that specific plans can be added or updated based on the outcomes.

Appendix A – Security Incident Categories

Category	Name	Description
CAT 1	Unauthorized Access to Systems	Confirmed unauthorized access to protected systems by either internal or external operators.
CAT 2	Unauthorized Release of Information	Confirmed unauthorized disclosure of DigiKnight Technologies, Inc. information, including the Personally Identifiable Information of employees, customers, and contractors.
CAT 3	Network Intrusion	Confirmed external network intrusion attempts such as DoS/DDoS attacks.
CAT 4	Malicious Code	Confirmed installation or attempted installation of foreign and malicious software onto company hardware. Includes the installation of malware, viruses, keyloggers, and any other malicious code.
CAT 5	External Reconnaissance	Confirmed external reconnaissance of DigiKnight Technologies, Inc. network vulnerabilities including but not limited to: port scanning, phishing attempts, and ping sweeps.
CAT 6	Password Breach or Privilege Abuse	Confirmed loss/theft/breach of passwords or authentication tokens to DigiKnight Technologies, Inc. property. Changes to local privilege settings of company devices outside of the stated change management process.
CAT 7	Information Security Policy Violation	Confirmed violation of any stated company information security policy.
CAT 8	Suspicious System Behavior or Failure	Confirmed unexpected network or system behavior including but not limited to: network degradation, increased bandwidth usage, excessive processor or memory use, and suspicious network requests.
CAT 9	Investigation	Unconfirmed, potentially malicious, incidents and anomalies within the DigiKnight Technologies, Inc. network.