Security Incident Response Plan

[SAMPLE]*

*Note: Incident Response Plans are highly customized for individual companies/institutions and should not be adopted without significant revision. Please contact Steve Cosentino: steve.cosentino@stinson.com for assistance.

Date Approved: <date>

Contents

Description 5
Purpose 5
Scope 5
Definitions 5
Information Security Incident Roles and Responsibilities 7
High Level Process 10
Identification 10
Analysis 10
Containment 10
Eradication 10
Recovery 10
Lessons Learned 10
Detailed Process 11
Identification 11
Detect 11
Report 11
Analysis 12
Cyber Insurance 12
Incident Severities 13
Incident Categories 14
Containment 15
Forensics 15
Eradication 16

Recovery 17
Data Recovery 17
System Upgrades 17
Modify Policies and Procedures 17
Notification (All Countries/Regions) 17
Notification (European Union) 17
Notification (United States) 18
Reputation Repair 19
Lessons Learned (Post-Incident Activity) 20
Appendix A: Contact List 21
Appendix B: Card Brand Breach Requirements 22
Appendix C: German Federal Data Protection Act: Section 42a 23
Appendix D: EU General Data Protection Regulation (EU-GDPR) Article 33 24
Appendix E: EU General Data Protection Regulation (EU-GDPR) Article 34 25
Appendix F 26
Related Policies 26
Related PCI Requirements 26
Related Controls 26
Functional Area 26
Process Owner 26
Contributors 26
Reviewer 26
Descriptions for Each Section in this Document 26

Description

This document describes the overall plan for information security incident response globally. The plan is derived from industry standards (ISO/IEC 27035:2011, PCI-DSS v3.2 and NIST 800-61) and applicable data privacy regulation(s) (e.g., BDSG in Germany, GDPR in the EU).

Each phase is described in detail below. Note that these are not necessarily chronological steps. Depending on the incident, it may be necessary to invoke several of these elements simultaneously. Also, this information should not be interpreted as a substitute for sound business discretion and decision-making depending on the particular facts of the incident and the affected parties.

Purpose

The primary goal is to limit the impact of an information security incident to customers, partners, employees and [Company] itself. This requires timely action and a coordinated approach with the parties involved.

Scope

- All locations
- All employees
- All contractors
- All third parties
- [Company] may experience numerous events over time, but they may never reach the level of a data breach. This plan covers incidents and data breaches. It does not cover events. See below for definitions.

Definitions

Event – The National Institute of Standards and Technology (NIST) defines an event as "any observable occurrence in a system or network," such as a server receiving a request for a web page, a user sending an e-mail message, or a firewall blocking an attempt to make a connection.

Incident – A security incident is an event that violates an organization's security policies and procedures. Verizon's 2016 Data Breach Investigations Report defines an incident as a "security event that compromises the integrity, confidentiality or availability of an information asset."

Breach (aka **Data Breach** or **Personal Data Breach**) – An incident resulting in the unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, and integrity of personal data.

Data breaches may require notification to the affected individuals, regulatory authorities, credit reporting agencies or the media. Additionally, contractual obligations require notice to business clients if the incident affected clients' employees or customers.

Personal Data (aka **Personally Identifiable Information** or **PII**) – In the United States personal data is sometimes defined as an individual's first name or first initial and last name plus one or more of the following: SSN, Drivers License, State ID, Account number, Credit Card or Debit card number combined with the security code, PIN, or password needed to access an account. State laws vary on the definition of PII and legal counsel should be consulted regarding the precise definitions that may apply in an Incident.

The European Union defines personal data as "any information relating to an identified or identifiable natural person." An identifiable person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data (e.g., IP address, MAC address), online identifier or one of more factors specific to the physical, physialogical, genetic, mental, economic, cultural or social identity of that person.

Anonymization (aka **Depersonalization**) – the process of turning data into a form which does not identify individuals and where identification is not likely to take place.

Pseudonymization – the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person.

Information Security Incident Roles and Responsibilities

As an incident progresses the core team will engage additional internal and external parties as deemed appropriate. The following table describes the expectations of the core team. It may not be comprehensive, but for those who are new to the process or aren't engaged often it serves as a reminder of why they are being asked to participate in an incident.

Role	Responsibility	Trigger
Information Security Incident Response Team (ISIRT) – the "Core Team"	1. Act as the lead function to investigate and coordinate incidents 2. Take appropriate steps to help contain and control the systems affected in an incident 3. Maintain inventory of incidents 4. Report incidents to the appropriate personnel 5. Act as the lead function to coordinate lessons learned and tests of this plan	Engaged in all information security incidents.
Legal	1. Provide legal support and expertise to the ISIRT 2. Establish privilege over investigations 3. Determine notification requirements 4. Determine possible legal liabilities and duties 5. Communicating with law enforcement (as necessary) 6. Notify government entities (as necessary)	Legal is triggered when the core team determines the incident could require notification, privilege regarding the investigation and remediation steps is desired, or if legal action is a possibility.
IT	1. Provide IT support and expertise to the ISIRT 2. Take appropriate steps to help contain and control the systems affected in a security incident and preserve information that may be helpful during the investigation	IT is triggered when the incident involves a system they support or have expertise on.
Information Security Operations	1. Provide information security operations support and expertise to the ISIRT 2. Taking appropriate steps to help contain and control the systems affected in an information security incident	When the incident involves a system they support or the ISIRT needs their expertise to advise and take action to contain and eradicate an incident.
Insurance	1. Provide cyber-insurance related support and expertise to the ISIRT 2. Identify if/when the insurance carrier should be engaged 3. Coordinate as the main point of contact with cyber-insurance provider 4. Submit claim(s) (as necessary) 5. Identify the requirements needed to meet the insurance provider's requirements to qualify for claim(s)	The insurance team is always informed of an incident.
Communications	1. Communicate (as necessary) with the media or outside sources 2. Communicate (as necessary) with employees and stakeholders	Communications is triggered when the incident involves the media or some public forum or when it involves internal resources.

Role	Responsibility	Trigger
Physical Security	1. Communicate details to the ISIRT when an incident occurs 2. Provide safety and security support	Physical security is triggered when the incident involves the safety of individuals, the preservation of evidence, or the ISIRT needs their expertise to advise and take action to contain and eradicate an incident.
Help Desk	1. Collect information and start filling out the Information Security Incident Report 2. Communicate the report to the core members of the ISIRT immediately 3. Direct any future inquiries to the ISIRT team 4. No information should be communicated inside or outside of [Company] unless it has been approved by the ISIRT	Help Desk is triggered when a potential incident is identified or if they need to respond to calls regarding the incident.
Data Protection Officer (DPO)	1. Provide data privacy support and expertise to the ISIRT 2. Act as the main point of contact for their area/location	The DPO is triggered when there is a potential data privacy related incident

Executive Leadership
Incident Lead
Sales
Marketing
Legal
Customer Service
IT
HR
Physical Security
Insurance
Compliance
Help Desk
Communications
Security/Data Privacy

High Level Process

An **Information Security Incident** is defined as one or more unwanted or unexpected security events that could very likely compromise the security of information and weaken or impair business operation. There are a number of steps taken to respond to an incident. The following describes each step as part of the overall process. Note they are not always followed in sequence and sometimes may occur at the same time.

Identification

Any available information is captured and shared with the incident response core team (ISIRT).

Analysis

The core team analyzes the information and determines if an incident has occurred. They determine if others need to be included depending on the situation.

Containment

As soon as the incident response team has analyzed the situation they determine what needs to be done to contain the incident so no further harm is done.

Eradication

The incident response team identifies the steps required to clean up the incident (i.e., remove malware, notify customers, etc.) and tracks them until complete.

Recovery

Once the incident has been contained and the cause eradicated, the team identifies and tracks recovery of any systems affected or business processes that need to be modified to prevent it from occurring again.

Lessons Learned

The incident response team periodically reviews past incidents to identify opportunity areas to grow and mature the process. It also includes periodic table top exercizes to practice for a breach the team has not experienced.

Detailed Process

Identification

Detect

There are a number of ways an incident can be identified.

Possible sources could include the following:

- Users/Employees
- IT Operations (including automated threat detection)
- Help Desk
- Social Media (Facebook, twitter, etc.)
- Mass Media (newspaper, bloggers, television, etc.)
- Websites (defacement archive sites, public information security websites, etc.)
- Any suspicion of potential cardholder data compromise could be reported to the payment brands by: law enforcement or issuing banks
- Managed Service Providers (ISP's, suppliers, etc.)
- Contact from white-hat or black-hat individuals
- Data Protection Officers

This is not a comprehensive list, but points out the wide variety of communication vehicles which exist and why it's important they all funnel through the Help Desk.

The moment an incident has been confirmed by ISIRT is the starting point to comply with several requirements governments and payment card brands have defined.

Report

Regardless of origin, all information security events/incidents must be funneled through the Help Desk extension _____. It runs 24/7/365 and is the central point of contact before ISIRT is engaged.

[INSERT LINK TO HELP DESK REFERENCE PAGE]

Analysis

ISIRT analyzes the information provided to them and determines if an incident has occurred, what severity and category it is, and who else needs to be included depending on the situation.

Verify Breach:

To determine whether Personal Information has been acquired or accessed, or is reasonably believed to have been acquired or accessed, by an unauthorized person as a result of a breach, [Company] will consider the following factors, among others:

- An indication the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other electronic data-storage device, containing relevant Personal Information.
- An indication that the information has been downloaded or copied by an unauthorized person, or was made available to unauthorized third parties for a meaningful period of time.
- An indication that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported (i.e., consumer or employee complaints).
- An indication that the information was accessed by individuals without permission, accessed for impermissible purposes, or that otherwise exceeded their authority to access or use such information (e.g., reviewing HR records for non-[Company] purposes).

Cyber Insurance

The ISIRT notifies the insurance risk management point of contact immediately in order for [Company] to take advantage of insurance (if appropriate).

Incident Severities

The following severity levels (SEV 1-4) are defined by _____ and are in line with the [Company] IME definitions of severity.

Severity Level & Response Time	Criticality Level Definition	Incident Categories	Ongoing Response	Ongoing Communication Requirement
Severity Level 1 (Critical) **One (1) Hour**	Events with "substantial security context" affecting numerous assets or representing a highly significant threat to the availability or integrity of the environment. Critical events often pose an immediate threat to the environment and are typically not mitigated by the organization's security controls.	• (CAT 1) Unauthorized Access or Changes to Information Systems • (CAT 2) Unauthorized Release of/or Disclosure of Information • (CAT 3) Network Intrusion • (CAT 4) Malicious Code (Widespread)	**Critical Phase** Threat Analyst assigned to work case on 24x7x365 basis. **Resolution Phase** Threat Analyst assigned to work on case during normal business hours.	Case update sent to appropriate parties on an hourly basis during critical phase.
Severity Level 2 (High) **Four (4) Hours**	Events with "substantial security context" affecting numerous assets or representing a highly significant threat to the availability or integrity of the environment. Critical events often pose an immediate threat to the environment and are typically not mitigated by the organization's security controls.	• (CAT 4) Malicious Code • (CAT 5) Reconnaissance (Widespread) • (CAT 6) Password Changes or Privilege Abuse	**Critical Phase** Threat Analyst assigned to work case on 24x7x365 basis. **Resolution Phase** Threat Analyst assigned to work on case during normal business hours.	Case update sent to appropriate parties on an hourly basis during critical phase.
Severity Level 3 (Medium) **One (1) Day**	Events affecting few assets or a single asset with a notable security context that may affect the availability or integrity of the environment.	• (CAT 0) Exercise / Network Defense Testing • (CAT 5) Reconnaissance • (CAT 8) Suspicious System Behavior or Failure	**Critical Phase** Case is worked as time/resources are available. **Resolution Phase** Case is worked as time/resources are available.	Case update sent to appropriate parties on an hourly basis during critical phase.
Severity Level 4 (Low) **One (1) Day**	Events affecting few assets or a single asset with minimal security context that may affect the availability or integrity of the environment.	• (CAT 7) Improper Use / Policy Violation • (CAT 9) Investigation	**Critical Phase** Case is worked as time / resources are available. **Resolution Phase** Case is worked as time / resources are available.	Case update sent to appropriate parties on an hourly basis during critical phase.

Incident Categories

Security incidents can be categorized as one of the 10 types as follows:

Category	Name	Description
CAT 0	**Exercise / Network Defense Testing**	This category is used during exercises and approved activity testing of internal/external network defenses or responses, such as penetration testing.
CAT 1	**Unauthorized Access or Change to Information / Systems**	Unauthorized access from internal and external sources to information and systems. Any unauthorized changes to file system, including media, through insertion, modification or deletion. For example, changes to standard operating environments (SOEs), addition of executables or the modification of an executable's configuration.
CAT 2	**Unauthorized Release of or Disclosure of Information**	Unauthorized release or disclosure of [Company] information, to include Personally Identifiable Information (PII), Intellectual Property, and other sensitive data to an unknown environment. Data exfiltration.
CAT 3	**Network Intrusion**	Intrusion specifically targeting client's internal infrastructure. This includes but is not limited to: • denial-of-service (DoS)/distributed denial-of-service (DDoS) • website defacements • brute force attempts
CAT 4	**Malicious Code**	Installation or attempted installation of software (e.g., virus, worm, Trojan Horse, key logger, bot, or other code-based malicious entity) designed and / or deployed by malicious actors with the intent of infecting an operating system or application.
CAT 5	**Reconnaissance**	Scans/Probes of client infrastructure with the intent to gain information used to characterize information systems, applications, networks, and users that may be used in follow-on attacks. • vulnerability scanning • port scanning • ping sweeps • phishing attempts • spam • packet sniffing
CAT 6	**Password Changes or Privilege Abuse**	Sharing/stealing/loss of passwords or other authentication token. Changes to privilege use settings on stand-alone or networked equipment including network profiles, local user or device configuration files that have not been approved through the client's change management process.
CAT 7	**Improper Use/ Policy Violation**	Any violation of information security policy.
CAT 8	**Suspicious Systems Behavior or Failure**	Unknown network activities affecting/degrading network performance with increased network bandwidth usage and decreased response time, using excessive CPU, increased suspicious network requests or increased Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) alerts leading to application crashes. This also includes silent log sources and missing heartbeats.
CAT 9	**Investigation**	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting analyst to warrant further review.

Containment

The following describes the protocol for all compromised systems during an information security incident. They must be followed until ISIRT determines it's no longer necessary:

- Do not access or alter compromised systems
  - Do not log on to the machine
  - Do not change passwords
  - Do not log in as ROOT, Administrator, or any other privileged account
- Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug network cable).
- Preserve logs and electronic evidence.
- Log all actions taken.
- Monitor all affected systems and alert on suspicious behavior.
- If using a wireless network, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection (with the exception of any systems believed to be compromised).
- Disable user accounts or change passwords.

Forensics

Forensics involves the identification, preservation, and analysis of potential evidence and documentation related to a data breach. For credit card related breaches, contractually the card brands in consultation with the bank may determine whether an independent forensic investigation is required.

In the event ISIRT requires a forensic analysis, the following should be considered:

1. Make efforts to prevent additional users from accessing affected machines or media
2. Consider volatility of evidence (i.e., the likelihood that evidence will be destroyed, overwritten or erased.)
3. Store collected information in a secure environment
4. Remember "Best Evidence Rule" -- courts prefer the original evidence where possible
5. Consider potential evidence from a variety of sources and media, including people
6. Maintain documentation of all containment, remediation and notification activities
   a. May need to be made available to regulatory bodies or auditors in the future
7. Preserving Chain of Custody
   a. Provides accountability
   b. Isolates chances for tampering of evidence
   c. Must account for all persons who handled or who had access to the evidence in question. Should include:
      i. Who initially acquired the evidence, and who acquired the evidence throughout the process of detection/assessment/investigation
      ii. When and where the evidence was collected
      iii. Identification of each piece of evidence
8. Where outside service provider(s) are involved, it is of paramount importance to communicate need for preservation of forensic evidence (especially Chain of Custody) in the event of a data breach.

Eradication

Once the incident has been contained (and where deemed necessary, a forensic investigation), eradication and recovery must be carefully executed. Failing to clean all affected systems prior to returning to operations may allow the attacker to return to their initial state of compromise and instantiate another incident.

Recovery

Factors to consider in the Recovery phase. Not in any particular order.

1. **Data Recovery**
2. **System Upgrades**
3. **Modify Policies and Procedures**
4. **Notification**
5. **Reputation Repair**

Data Recovery

Invoke Disaster Recovery and/or Business Continuity Plans as appropriate.

System Upgrades

- Patch vulnerabilities
- Upgrade complete versions where patches aren't sufficient
- Improve the secure configuration of systems
- Improve the architecture of systems

Modify Policies and Procedures

- Make changes to policies, standards and procedures to prevent further damage or breaches.

Notification (All Countries/Regions)

Notification requirements will be determined by the ISIRT.

Criteria for Notification:

Whether notification is required, its format, and its timing will be determined by ISIRT in cooperation with legal counsel and others as determined by ISIRT.

Notification (European Union)

Germany

Germany has enacted the Federal Data Protection Act (BDSG) to protect the individual against his right to privacy being impaired through the handling of his personal data. Per BDSG Section 42a (to be replaced with GDPR Article 33/34 in 2018) "data subjects shall be informed as soon as appropriate measures to safeguard the data have been taken and notification would no longer endanger criminal prosecution."

The following types of specific information defines whether a data breach has occurred and notification is required per the BDSG:

1. special types of personal data (Section 3 (9)),
2. personal data subject to professional secrecy,
3. personal data related to criminal offences or administrative offences or the suspicion of punishable actions or administrative offences, or
4. personal data concerning bank or credit card accounts

Data covered by the German Telemedia Act needs to be consider -> example: Username and Password.

Prior to May 2018, the Data Protection Authority of Bavaria requires an online form to be completed by the company DPO. The link can be found here: https://www.lda.bayern.de/en/data_breach.html#top

German is the national language. Any notification in Germany must be in the German language.

Notification (United States)

Notification in the United States is governed by state and federal laws. Legal counsel is responsible for providing final advice in this matter.

Contacting Law Enforcement:

If [Company] reasonably believes that a breach has occurred, the ISIRT will designate a single point of contact. The point of contact will immediately report the incident to the appropriate law enforcement agencies, if required or if [Company] decides it is appropriate.

- The point of contact should inform the law enforcement official in charge of the investigation that it intends to provide (or arrange for the provision of) Notice to affected individuals in the most expedient time possible and without unreasonable delay. If the law enforcement official in charge informs [Company] that giving Notice at that time would impede a criminal investigation, then:
    - The point of contact should ask the official how soon [Company] may notify the affected individuals without impeding the criminal investigation, and will document this request and the response; and
    - Legal and Public Relations (for breaches affecting non-employees) and/or Human Resources (for breaches affecting employees) should be prepared to send the Notices immediately upon being so authorized by law enforcement officials.

Notification to Consumer:

A sample consumer notice letter ("SR-12 Sample Consumer Notification Letter") is maintained along with this process document. The exact wording of the letter need not be followed and instead should be determined by ISIRT in consultation with legal counsel and others as requested by ISIRT

Form and Style of the Notice:

The Notice must be written in a clear manner, using easy-to-understand language. The Notice should be a stand-alone document, not combined as part of another mailing.

Means of Notification:

ISIRT will determine the proper means of communication including any use of vendors in consultation with legal counsel and others as requested by ISIRT.

Notification to States:

To the extent and as required by law, Legal will promptly provide written notification of the breach to relevant state governmental authorities.

Notification to Payment Card Issuers and Banks:

In instances in which Personal Information associated with a credit or debit card is reasonably believed to have been acquired or accessed by an unauthorized person, a designated point of contact from the ISIRT will notify the relevant payment card issuers, payment processor(s), and banks pursuant to any

contractual obligations that [Company] has with respect to the card issuers or banks, within the time period required by such contractual obligations (see Appendix A for contact information).

Notification to Payment Processor:

See Appendix A below for contact information.

Notification to Payment Card Issuers:

See Appendix A below for contact information.

Press

- To be handled by Public Relations with support from Legal (and other parties of ISIRT or business leaders as deemed necessary depending on the circumstances).

Internal-facing communications and talking points

a. Potential audience:
   i. Employees
   ii. Customer Service or Help Desk personnel
b. To be drafted by Legal and Public Relations with input and review from appropriate members of ISIRT and senior management.

Reputation Repair

Reparation of reputational harm and restoring consumer confidence, where applicable.

Lessons Learned (Post-Incident Activity)

A thorough analysis of how the incident was detected, notified, handled and contained should be performed when determined necessary by ISIRT, but at least annually. The incident plan should be updated according to the results of the analysis in order to improve monitoring alerts analysis, response times, and to optimize the incident response procedures.

Limited scope table top reviews are available as a service through our cyber insurance provider. The incident response team should take advantage of these services as appropriate.

The Information Security organization is responsible for staying current on any industry developments in the area of incident response or data breaches.

Appendix A: Contact List

Name	Phone	Email/Web	Trigger

Appendix B: Card Brand Breach Requirements

Requirement	American Express	Discover	JCB	MasterCard	VISA
Notification	Immediately	Immediately	Not specified	Within 24 hours of knowledge	Immediately
Forensic Investigation & Audit	Should be performed by a third party forensic investigator.	Not specified	Not specified	Should be performed by a data security firm acceptable to MasterCard.	Independent forensic investigation may be required at Visa and merchant bank's discretion. A QIRA (Qualified Incident Response Assessor) should perform the forensic investigation. An independent third party acceptable to VISA must conduct a security review after eradication / remediation.
Forensic Investigation Timeframe	Not specified	Not specified	Not specified	Within 72 hours of knowledge.	Within 3 business days of the reported compromise, an incident report should be provided to your merchant bank.
Compromised Account Reporting	Not specified	Not specified	Not specified	Use a text file (.txt) and expiration date in a MMYY format.	Provide all the compromised accounts within 10 business days.
Additional Requirements	Not specified	Not specified	Not specified	Weekly Status reports.	Specific report format.

Appendix C: German Federal Data Protection Act: Section 42a

Section 42a

Obligation to report unlawful access to data

If a private body as defined in Section 2 (4) or a public body as defined in Section 27 (1) first sentence No. 2 determines that

1. special types of personal data (Section 3 (9)),
2. personal data subject to professional secrecy,
3. personal data related to criminal offences or administrative offences or the suspicion of punishable actions or administrative offences, or
4. personal data concerning bank or credit card accounts

stored with that body have been unlawfully transferred or otherwise unlawfully revealed to third parties, with the threat of serious harm to the data subject's rights or legitimate interests, then in accordance with sentences 2 to 5 the body shall notify the responsible supervisory authority and the data subject without delay. The data subject shall be notified as soon as appropriate measures have been taken to protect the data and notification would no longer put criminal prosecution at risk. The notification for the data subjects shall describe the nature of the unlawful access and include recommendations for measures to minimize possible harm. The notification for the competent supervisory authority shall also describe possible harmful consequences of the unlawful access and measures taken by the body. Where notifying the data subjects would require unreasonable effort, in particular due to the large number of cases involved, such notification may be replaced by public advertisements of at least one-half page in at least two national daily newspapers, or by another equally effective measure for notifying the data subjects. A notification distributed by the body required to provide notification may be used against that body in criminal proceedings or in proceedings in accordance with the Administrative Offences Act, or against an associate of the body required to provide notification as defined in Section 52 (1) of the Code of Criminal Procedure only with the consent of the body required to provide notification.

Appendix D: EU General Data Protection Regulation (EU-GDPR) Article 33

EU General Data Protection Regulation (EU-GDPR)

Article 33 - Notification of a personal data breach to the supervisory authority

=> Article: 4

=> Recital: 75, 85, 87, 88

=> administrative fine: Art. 83 (4) lit a

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

=> Recital: 75

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Appendix E: EU General Data Protection Regulation (EU-GDPR) Article 34

EU General Data Protection Regulation (EU-GDPR)

Article 34 - Communication of a personal data breach to the data subject

=> Article: 4

=> Recital: 75, 86, 87, 88

=> administrative fine: Art. 83 (4) lit a

Opening clause!

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

=> Recital: 75

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Appendix F

Related Policies

- 16.0 Incident Management Policy

Related PCI Requirements

- 11.1.2, 12.5.3, 12.10, 12.10.1, 12.10.2, 12.10.3, 12.10.4, 12.10.5, 12.10.6

Related Controls

- 19.1 – 19.7

Functional Area

Information Security

Process Owner

Jeff L. Johnson

Contributors

- Sandra Stocker

Reviewer

<full name here>

Descriptions for Each Section in this Document

Description: The description section includes a high level executive overview of the reusable solution. Should be 1-2 paragraphs. Details are provided throughout the plan.

Purpose: Answers the question "Why does this plan exist?" What problem(s) are being solved? What risk(s) are being addressed?

Scope: What areas of [Company] are affected by this plan?

Process: Defines the steps (procedures) using process flows, swim lanes, and descriptions of each step.

Related Policies: Include the list of policies from the Information Security Policy and their specific sections this plan addresses.

Related PCI Requirements: Where applicable, include the specific controls that are met using this plan.

Related Controls: List the specific controls from the Computer Internet Security (CIS) Critical Security Controls (CSC) Top 20 Controls that are met using this plan.

Functional Area: Select the organizational functional area this plan will be operated by.

Process Owner: Who is the owner of this process? The owner identified here will be the primary contact for this plan, and will be responsible for ensuring that it is adhered to by the Functional Area.

Contributors: Who contributed to this plan?

Reviewer: Who was the final reviewer/approver of the plan?