Frontera Consulting

Security Breach Policy
[V0.1]

Table of Contents

Section I: Introduction

A. How to Use This Policy

In the event of a security breach which interferes with Frontera Consulting's ability to conduct business from one of its offices, this plan is to be used by the responsible individuals to coordinate the business recovery of their respective areas and/or departments. The plan is designed to contain, or provide reference to, all of the information that might be needed at the time of a business recovery.

Section I, Introduction, contains general statements about the policy. It also establishes responsibilities for enacting the recovery plan.

Section II, Security Breach Policy Strategy, describes the strategy that Frontera Consulting will control/implement to maintain business continuity in the event of a data security disruption. These decisions determine the content of the action plans, and if they change at any time, the plans should be changed accordingly.

Section III, Security Responsibilities, lists the security owners, who are assigned specific responsibilities, and procedures on how each of the team members is to be notified.

Section IV, Procedures, determines what activities and tasks are to be taken, in what order, and by whom in order to affect the recovery.

Section V, Appendices, contains all of the other information needed to carry out the plan. Other sections refer the reader to one or more Appendices to locate the information needed to carry out the Team Procedures steps.

B. Objectives

The objective of the Security Breach Policy is to coordinate recovery of critical business functions in managing and supporting the business recovery in the event of a security breach causing disruption or disaster. This can include , but is not limited to, stolen information, ransomware, password guessing, recording keystrokes, phishing attacks, malware or virus, or Distributed Denial of Service attacks (DDoS).

A security breach is defined as any data related event that targets company information, including but not limited to client data, employee data, financial data, and any other business relevant information that is not public knowledge, and interferes with the organization's ability to deliver essential business services.

A near miss is an event that does not result in a data breach, but which had the potential to do so. Examples of such events might include data that was misplaced

but found quickly internally or data that was sent out but was identified and returned.

C. Scope

The Security Breach Policy is limited in scope to recovery and business continuance from a serious disruption in activities due to a security breach of the Frontera Consulting's data. Unless otherwise modified, this policy does not address temporary interruptions of duration less than the time frames determined to be critical to business operations.

The scope of this policy is focused on identifying, reporting, containment, recovery, investigation, risk assessment, evaluation and response following a security data breach incident.

D. Security Breach Policy/Maintenance Responsibilities

Maintenance of Frontera's Security Breach Policy is the joint responsibility of the executive management team, HR & Operations, and the Data Protection Officer/ISMS.

The executive management team, with HR is responsible for:

1. Periodically reviewing the adequacy and appropriateness of its security protection strategy.
2. Assessing the impact of additions or changes to existing business functions, procedures, equipment, and facilities requirements.
3. Keeping recovery team personnel assignments current, taking into account promotions, transfers, and terminations.
4. Communicating all policy changes to the Data Protection Officer/ISMS so that the organization's Policy can be updated.

The Data Protection Officer is responsible for:

1. Ensuring that the business has an adequate process of identification, containment and response in case a near miss or a security breach happens, and also that this process is documented and distributed within the company.

E. Policy Testing Procedures and Responsibilities

Data Protection Office / Operations is responsible for ensuring the workability of their Security Breach Policy. This should be periodically verified by active or passive testing.

F. Policy Training Procedures and Responsibilities

HR is responsible for ensuring that the personnel who would carry out the Security Breach Policy are sufficiently aware of the policy's details. This may be accomplished in a number of ways including; practice exercises, participation in tests, and awareness programs conducted by the Data Protection Owner.

Section II: Security Breach Policy Strategy

A. Introduction

This section of the Policy describes the strategy devised to maintain business continuity in the event of a security breach.

This strategy would be invoked should Frontera Consulting be under a security breach threat or near miss.

B. Recovery Priorities

The strategy is to stop the effects of the security breach as soon as possible and recover critical business functions if they were affected. This can be possible if the priorities have been mapped out and the Data Protection Officer is aware of them and how to implement them.

The priorities in a security breach or near miss situation are to:

1. Stop any activity that could cause interference with business activities as soon as possible.
2. Report the data breach or the near miss event to the Data Protection Officer.
3. Data Protection Officer must investigate at once the occurrence and complete a risk assessment. [The investigation must take into consideration the type of data involved, its sensitivity, existence of controls (e.g. encryptions), what happens to the data (has it been lost, stolen, ransomware), whether the data could be put to any illegal or inappropriate use, data subject(s) affected by the breach, number of individuals involved and the potential effects on the data subject(s), and whether there are wider consequences of the breach.]
4. Mitigate breaches or limit the damage that breaches can cause.
5. Have advanced preparations to ensure that critical business functions can continue.
6. Have documented plans and procedures to ensure the quick, effective execution of recoverystrategies for critical business functions.

Section III: Security Responsibilities

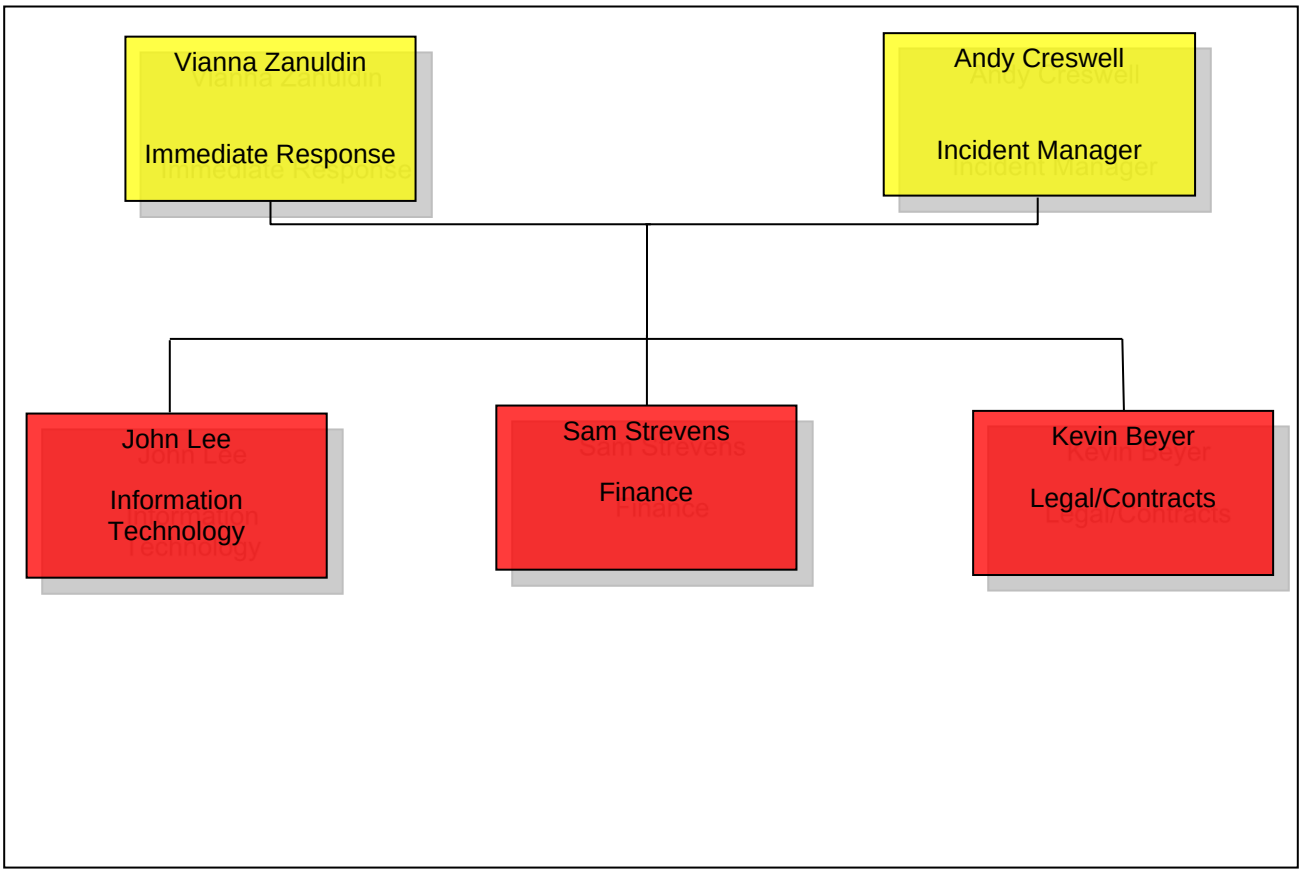
A. Purpose and Objective

This section of the plan identifies who will participate in the recovery process.

B. Personnel Notification

This section specifies how the team members are to be notified if the plan is to be put into effect by identifying who needs to be notified and who needs to take action

C. Team Responsibilities



Section IV: Procedure

A. Purpose and Objective

This section of the plan describes the specific activities and tasks that are to be carried out in the recovery process. Given the Security Breach Policy outlined in **Section II**, this section transforms those strategies into a very specific set of action activities and tasks according to recovery phase.

The Recovery Procedures are organized in the following order: recovery phase, activity within the phase, and task within the activity.

B. Activities and Tasks

The Data Protection Officer will be the one assessing and managing the incident.

In the event of a near miss or data breach, the strategy is to stop the flow of data as soon as possible, the damage is mitigated and the Data Protection Officer is assessing the overall risk of the breach.

1. Security Breach Occurrence

The Data Protection Officer must determine if the breach is still in progress and if so, must take the appropriate steps to minimize its effect.

TASKS:

1. Should a breach be suspected, immediately notify Security Manager and Operations Manager. Immediately log out of all applications, reset password, and run antivirus software. Types of breaches:

- malware
- phising attack
- ransomware
- virus
- password hack
- equipment theft of failure
- loss or theft of confidential data
- unauthorised disclosure of confidential data
- human error

2. After a security breach occurs, quickly assess the situation to determine whether if the breach is still occurring, and what can you do to minimse the effects of the breach.

3. Quickly assess whether any other employee has been potentially affected, and if there are multiple devices being affected by the breach. If you are unable to determine, take precautions to stop the breach on your own.

4. Depending upon the time of the security breach, personnel are instructed what to do (i.e.change passwords, enable 2FA, etc.)

2. Assessment

The Data Protection Officer, in liaison with relevant officer(s), must perform an initial assessment to establish the severity of the breach and who will take ownership of investigating the breach. This will establish the nature of the breach, the severity, and whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

TASKS:

1. Caution all personnel to avoid security risks as follows:
    - Do not open suspicious emails, messages, documents if these are coming from outside the organization and/or known contacts.
    - Do not disable 2FA.
    - Do not share logins, passwords, links, bank information or otherwise relevant data with members of the team, family, etc.
    - Report any suspicious activity as soon as possible, even if the impact is non-existent. This is classified as a near miss.

3. Notification and Distribution

The owner of the investigation, along with the Data Protection Officer, must establish who will be notified as part of the initial containment, and will inform the authorities, where appropriate.

TASKS:

Senior Management and Partners need to notify the Frontera employees on the risk encountered, type of breach, investigation process and results, as well as best practices and lessons learned after the incident.

This is done to ensure that similar breaches/near misses won't happen, as the employees would have been already educated on the topic.

4. Containment

In order to resolve the incident swiftly and with minimal impact, expert advice from various business functions, as well as external council if needed, will be required to determine the suitable course of action.

TASKS:

Following the internal recommendations from Senior Management and Partners, corrective actions need to be put in place on a case by case basis, depending on the security breach. If the Organisation needs outside council, this will be done by the Senior Management and the Partners in conjunction with external experitise on a case by case basis.

a) Vital Records Backup

All vital records for Frontera Consulting that would be affected by a facilities disruption are maintained and controlled within the cloud on OneDrive. These files are backed up and stored securely via Microsoft Office 365.

All vital documents are typically located in files within the Cloud and one OneDrive and the most current back-up copies are secure.

b) Restoration of Hardcopy Files, Forms, and Supplies

In the event of a security breach, critical data may be destroyed or inaccessible. In this case, the last backup of critical documents would be restored from OneDrive.

The following categories of information can be exposed to loss:

1. Any files stored on-site in file cabinets and control file rooms.
2. Information stored on local PC hard drives.
3. Received and un-opened mail.
4. Documents in offices, work cubes and files.

c) On-line Access to Frontera Consulting Computer Systems

In the event of a security breach, all Frontera Consulting departments are enabled to work remotely. All files and documents vital to daily operations are accessed via the cloud.

Appendix A – Incident Report Template

Security Incident – E-mail Phishing attack breach 18th August 2020

Date	20th Aug 2020
Type of incident	Phishing attack on Employees Office 360 account.
Issue:	0.1 Draft
Document Links	Frontera Security Policy Frontera C2C Incident Management plan IS27K ISMS Manual IS Incident Reporting Policy

REVISION HISTORY

Revision No.	Date	Reason for issue
1.0	1st February 2020	Template

Contents

Security Incident Template.docx