WORTHERS

DATA BREACH POLICY

Introduction

This document is intended to be used when an incident of some kind has occurred that affects the information security of Worthers Limited, including those potentially affecting personal data for which the organisation is a controller. It is intended to ensure a quick, effective and orderly response to an information security breach.

Purpose

This policy sets out in detail how the organisation will initially react to an information security incident (which may or may not affect personal data) and manage it going forward.

The procedures set out in this document should be used only as guidance as the exact nature of an incident and its impact cannot be predicted with any degree of certainty and so a good degree of common sense will be used when deciding the actions to take. It is intended that the structures set out here will prove useful in allowing the correct actions to be taken more quickly and based on more accurate information.

The following areas of the GDPR are addressed by this document:

Article 33 – Notification of a data breach to the supervisory authority
Article 34 – Communication of a personal data breach to the data subject

Objectives

The objectives of this incident response procedure are to:

- provide a concise overview of how Worthers Limited will respond to an incident
- set out who will respond to an incident and their roles and responsibilities
- describe the facilities that are in place to help with the management of the incident
- define how decisions will be taken with regard to our response to an incident
- explain how communication within the organisation and with external parties will be handled
- provide contact details for key people and external agencies
- define what will happen once the incident is resolved and the responders are stood down

Definitions

A personal data breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Data breach incident – this can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data subject – the client who has personal data is held with Worthers Limited.

Incident Response Flowchart

The flow of the incident response procedure is shown in the diagram below.

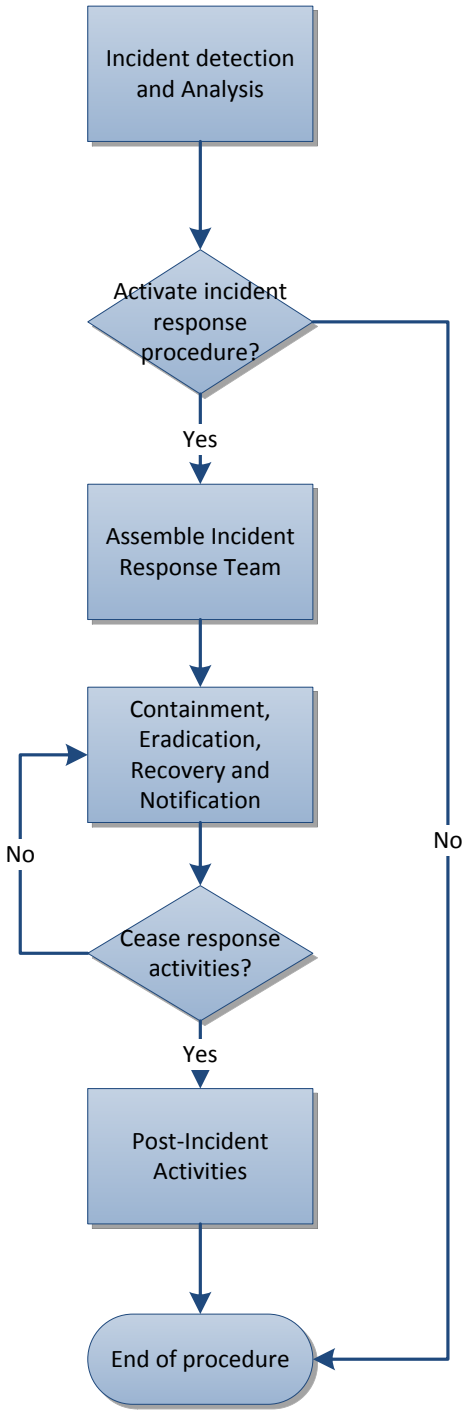

Figure 1 – Incident response flowchart

These steps are explained in more detail in the rest of this procedure.

Incident Detection and Analysis

An incident may be initially detected in a wide variety of ways and through a number of different sources, depending on the nature and location of the incident. Some incidents may be self-detected via software tools used within Worthers Limited or by employees noticing unusual activity. Others may be notified by a third party such as a customer, supplier or law enforcement agency who has become aware of a breach perhaps because the stolen information has been used in some way for malicious purposes.

It is not unusual for there to be a delay between the origin of the incident and its actual detection; one of the objectives of a proactive approach to information security is to reduce this time period. The most important factor is that the incident response procedure will be started as quickly as possible after detection so that an effective response can be given.

Once the incident has been detected, an initial impact assessment will be carried out in order to decide the appropriate response.

This impact assessment will estimate:

- The extent of the impact on IT infrastructure including computers, networks, equipment and accommodation
- The information assets (including personal data) that may be at risk or have been compromised
- The likely duration of the incident i.e. when it may have begun
- The business units affected and the extent of the impact to them
- For breaches affecting personal data, the degree of risk to the rights and freedoms of the data subjects
- Initial indication of the likely cause of the incident

This information will be documented so that a clear time-based understanding of the situation as it emerges is available for current use and later review.

A list of the information assets (including personal data), business activities, products, services, teams and supporting processes that may have been affected by the incident will be created together with an assessment of the extent of the impact.

As a result of this initial analysis, the management team will act as an Incident Response Team (IRT) and assess whether the Incident Response Procedure should be activated.

Activation of the Incident Response Procedure

Once notified of an incident the Team Leader will decide whether the scale and actual or potential impact of the incident justifies the activation of the Incident Response Procedure.

Guidelines for whether a formal incident response will be initiated for any particular incident of which the Team Leader has been notified are if any of the following apply:

- There is significant actual or potential loss of classified information, including personal data
- There is significant actual or potential disruption to business operations
- There is significant risk to business reputation
- Any other situation which may cause significant impact to the organisation

In the event of disagreement or uncertainty about whether or not to activate an incident response the decision of the Team Leader will be final.

If it is decided not to activate the procedure then a plan will be created to allow for a lower level response to the incident within normal management channels. This may involve the invocation of relevant procedures at a local level.

If the incident warrants the activation of the IR procedure the Team Leader will start the process.

Assembly of Incident Response Team

Once the decision has been made to activate the incident response procedure, the Team Leader (or deputy) will ensure that the Incident Response Team is assembled and made aware of the nature of the incident.

The members of the team are as follows:
Peter Worthington (Team leader)
Kate Worthington
Ben Hull
Chris Lugg

The responsibilities of the roles within the incident response team are as follows:

Team Leader

- Decides whether or not to initiate a response
- Assembles the incident response team
- Overall management of the incident response team
- Final decision maker in cases of disagreement
- Prepares for meetings and takes record of actions and decisions
- Briefs team members on latest status on their return to the workplace
- Facilitates communication via email, fax, telephone or other methods
- Monitors external information feeds such as news
- Contributes to decision-making based on knowledge of business operations, products and services
- Helps to assess likely impact on customers of the organisation
- Assesses the risk to life and limb of the incident
- Ensures that legal responsibilities for health and safety are met at all times

- Liaises with emergency services such as police, fire and medical
- Considers environmental issues with respect to the incident
- Assesses and advises on HR policy and employment contract matters
- Represents the interests of organisation employees
- Advises on capability and disciplinary issues
- Responsible for ensuring internal communications are effective
- Decides the level, frequency and content of communications with external parties such as the media
- Defines approach to keeping affected parties informed e.g. customers, shareholders

Other roles for all other members

- Assess the extent and impact of the incident
- Provides first-person account of the situation
- Liaises on an on-going basis to provide updates and answer any questions required for decision-making by the IRT
- Provide input on technology-related issues
- Assist with impact assessment
- Assumes other responsibilities as the team leader designates.

Incident Management, Monitoring and Communication

Once an appropriate response to the incident has been identified, the IRT will manage the overall response, monitor the status of the incident and ensure effective communication is taking place at all levels.

Regular IRT meetings will be held at an appropriate frequency decided by the Team Leader. The purpose of these meetings is to ensure that incident management resources are managed effectively and that key decisions are made promptly, based on adequate information. Each meeting will be minuted.

Communication Procedures

Effective communication will be maintained between all parties involved in the incident response.

The primary means of communication during an incident will initially be email, telephone, both landline and mobile. Also we may post applicable summary details on a web page.

The following guidelines should be followed in all communications:

All communications will be clearly and accurately recorded.

Communication to the Data Protection Supervisory Authority

It is a requirement of the EU General Data Protection Regulation 2016 (GDPR) that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisory authority without undue delay and where feasible, within 72 hours of becoming aware of it. The Worthers Limited *Personal Data Breach Notification Procedure* will be used for this purpose. In the event that the 72-hour target is not met, reasons for the delay will be given.

Communication with Personal Data Subjects

Where an incident affects personal data, a decision will be taken by the IRT regarding the extent, timing and content of communication with data subjects. The EU GDPR requires that communication must happen "without undue delay" if the breach is likely to result in "a high risk to the rights and freedoms of natural persons".
The Worthers Limited *Personal Data Breach Notification Procedure* will be used for this purpose.

Other External Communication

Depending on the incident there may be a variety of external parties that will be communicated with during the course of the response. This information will be managed so that it is timely and accurate.

Calls that are not from agencies directly involved in the incident response (such as the media) will be passed to the member of the IRT responsible for communications.

There may be a number of external parties who, whilst not directly involved in the incident, may be affected by it and may need to be alerted to this fact. These may include:

- Customers
- Suppliers
- Shareholders
- Regulatory bodies

The IRT will make a list of such interested parties and define the message that is to be given to them.

Interested parties who have not been alerted by the IRT may call to obtain information about the incident and its effects. These calls will be recorded in a message log and passed on to the Team Leader.

Communication with the Media

In general the communication strategy with respect to the media will be to issue updates via the IRT (when necessary) in the form of pre-written press releases and in exceptional circumstances a press conference. No members of staff will give an interview with the media unless this is pre-authorised by the IRT. Personal data will be protected at all times.

Incident Containment, Eradication, Recovery and Notification

Containment

The first step will be to try to stop the incident getting any worse i.e. contain it. In the case of a virus outbreak this may entail disconnecting the affected parts of the network; for a hacking attack it may involve disabling certain profiles or ports on the firewall or perhaps even disconnecting the internal network from the Internet altogether. The specific actions to be performed will depend on the circumstances of the incident.

Note: if it is judged to be likely that digital evidence will need to be collected that will later be used in court, precautions will be taken to ensure that such evidence remains admissible.

Particularly (but not exclusively) if foul play is suspected in the incident, accurate records will be kept of the actions taken and the evidence gathered in line with digital forensics guidelines. The main principles of these guidelines are as follows:

Next, a clear picture of what has happened will be established. The extent of the incident and the knock on implications will be ascertained before any kind of containment action can be taken.

Audit logs may be examined to piece together the sequence of events; care will be taken that only secure copies of logs that have not been tampered with are used.

Eradication

Actions to fix the damage caused by the incident, such as deleting malware, will be put through the change management process (as an emergency change if necessary). These actions would be aimed at fixing the current cause and preventing the incident from re-occurring. Any vulnerabilities that have been exploited as part of the incident will be identified.

Depending on the type of incident, eradication may sometimes be unnecessary.

Recovery

During the recovery stage, systems will be restored back to their pre-incident condition, although necessary actions will then be performed to address any vulnerabilities that were

exploited as part of the incident. This may involve activities such as installing patches, changing passwords, hardening servers and amending procedures.

Notification

The notification of an information security incident and resulting loss of data is a sensitive issue that will be handled carefully and with full management approval. The IRT will decide, based on legal and other expert advice and as full an understanding of the impact of the incident as possible, what notification is required and the form that it will take.

Worthers Limited will always comply in full with applicable legal and regulatory requirements regarding incident notification and will carefully assess any offerings to be made to parties that may be impacted by the incident, such as credit monitoring services.

Records collected as part of the incident response may be required as part of any resulting investigations by relevant regulatory bodies and Worthers Limited will cooperate in full with such proceedings.

Post-Incident Activity

The Team Leader will decide, based on the latest information the point at which response activities should be ceased and the IRT stood down. Note that the recovery and execution of plans may continue beyond this point but under less formal management control.

This decision will be up to the Team Leader's judgement but will be based upon the following criteria:

- The situation has been fully resolved or is reasonably stable
- The pace of change of the situation has slowed to a point where few decisions are required
- The appropriate response is well underway and recovery plans are progressing to schedule
- The degree of risk to the business has lessened to an acceptable point
- Immediate legal and regulatory responsibilities have been fulfilled

If recovery from the incident is on-going the Team Leader will define the next actions to be taken. These may include:

- Informing all involved parties that the IRT is standing down
- Ensuring that all documentation of the incident is secured

All actions taken as part of standing down will be recorded.

After the IRT has been stood down the Team Leader will hold a debrief of all members ideally within 24 hours. The relevant records of the incident will be examined by the IRT to

ensure that they reflect actual events and represent a complete and accurate record of the incident.

Any immediate comments or feedback from the team will be recorded.

A more formal post-incident review will be held at a time to be decided by top management according to the magnitude and nature of the incident.