EX Networks Limited

Data Breach Response Policy

Issued: 07/05/2018

Version 2.0

https://www.exn.uk/resources/

Data Breach Response Policy

This document informs you of our policy regarding data breaches and establishes the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritisation of the incidents), as well as reporting, remediation, and feedback mechanisms.

The policy shall be well publicised and made easily available to all clients and EX Networks staff who use or access our Services and whose duties involve data privacy and security protection

Contents

Background

EX Networks intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how EX Networks' established culture of openness, trust and integrity should respond to such activity.

EX Networks are committed to protecting EX Networks' employees, partners, customers and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

This policy mandates that any individual who suspects that a theft, breach or exposure of EX Networks Protected Data or EX Networks Sensitive Data has occurred must immediately provide a description of what occurred via our contact page

https://www.exn.uk/contact-us/

This address, phone number and website are monitored by EX Networks. We will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, EX Networks will follow the appropriate procedure in place.

Scope

This policy applies to all who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Personally Identifiable Information (PII) or Protected Health Information (PHI) of EX Networks' members.

Policy Confirmed theft, data breach or exposure of Protected Data or Sensitive Data

As soon as a theft, data breach or exposure containing EX Networks Protected Data or EX Networks Sensitive Data is identified, the process of removing all access to that resource will begin.

The Managing Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- Network Infrastructure
- Systems Infrastructure
- Finance (if applicable)
- Legal (if applicable)
- Customer Services (if applicable)
- Human Resources
- The affected unit, or department or Customer that uses the involved system or output or whose data may have been breached or exposed
- Additional departments and external parties based on the data type involved, additional individuals as deemed necessary by the Managing Director

The Managing Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyse the breach or exposure to determine the root cause.

Work with Forensic Investigators

If required EX Networks will provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external

individuals and/or organizations impacted; and analyse the breach or exposure to determine the root cause.

Develop a communication plan

EX Networks communications, legal and human resources departments will decide how to communicate the breach to:

- internal employees,
- the public,
- Customer(s),
- those directly affected.

Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the EX Networks team that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any member of the EX Networks management team in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is the member of the EX Networks team, designated by the Managing Director who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the EX Networks team to the extent they have authorised access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Management and shall include, but will not be limited to, the following departments or their representatives: Network Infrastructure, Systems Infrastructure, Finance, Legal, Customer Services, Human Resources.

Enforcement

Any EX Networks employees found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their Services terminated.

Definitions

Plain text – Unencrypted data.

Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

Protected Health Information (PHI) - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity) and can be linked to a specific individual.

Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered.

Protected data - See PII and PHI.

Information Resource - The data and information assets of an organisation, department or unit.

Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

Sensitive data - Data that is encrypted or in plain text that contains PII or PHI data. See PII and PHI above.

References

Information Commissioner:

https://ico.org.uk/media/1562/guidance_on_data_security_breach_management.pdf

Data Breach Reporting Template

	Report prepared by: Date: On behalf of:	
1	Summary of the event and circumstances	
2	Type and amount of personal data	
3	Actions taken by recipient when they inadvertently received the information	
4	Actions taken to retrieve information and respond to the breach	
5	Procedures / instructions in place to minimise risks to security of data	
6	Breach of procedure/policy by staff member or customer	
7	Details of notification to affected data subject Has a complaint received from Data Subject?	

8	Details of Data Protection training provided:	
9	Procedure changes to reduce risks of future data loss	
10	Conclusion	