

Data Breach Policy & Procedures - Customer

(ISO 27001:2022 Organisational Controls – Clause 5.24)

Author	Greg Nott
Version	2.0
Date Created	02/11/2023
Last Update Date	24/05/2024
Document Control	Released
Document ID	231102-IMS-POL-DataBreachCustomer-V2
Security Classification	Public

Table of Contents

Data Breach Policy & Procedures - Customer	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Purpose.....	4
Data Security and Breach Requirements	4
Breach Monitoring & Reporting.....	4
Breach Incident Procedures.....	4
Identification of an Incident.....	4
Breach Recording.....	5
Breach Risk Assessment.....	5
Breach Notifications.....	5
Responsibilities	5

Approval

Author	Issue	Approved By	Date
Paul Langan	1.0	Simon Naylor	02-Nov-23
Greg Nott	2.0	Wayne James	23-May-24

Review

Reviewer	Review Criteria	Issue	Date
Greg Nott	ISO 27001:2022	1.0	02-Nov-23
Paul Langan	Review & Rebrand	2.0	23-May-24

Change History

Author	Change	Issue	Date
Paul Langan	Creation	1.0	02-Nov-23
Greg Nott	Review & Rebrand	2.0	23-May-24

Associated Documents

Document	Version
230918-SEC-PRO-AROCriticalSecurityIncidentResponseCustomer	2.0

Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and describes the Data Breach Policy & Procedures adopted by ARO.

- ISO 27001:2022 – Information Security Management Systems
 - ISO 27017:2015 – Code of Practice for Cloud Services
 - ISO 27018:2020 – Code of Practice of Personally Identifiable Information (PII)
- ISO 9001:2015 – Quality Management System
- DSPT (Data Security and Protection Toolkit) for the NHS.
- Cyber Essentials Plus

Purpose

The purpose of this policy is to provide the objectives and procedures regarding data breaches involving personal information within a supported customers environment.

This document should be read in conjunction with the ARO Critical Security Incident Response Procedure – Customer.

Data Security and Breach Requirements

AROs definition of a personal data breach for the purposes of this policy is any breach of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

During application of the Critical Security Incident Response Procedure, consideration must also be given to the customers own definition of personal data, or other sensitive information types. As communication is maintained with the customer information relating to impacted locations and/or contents should be shared to allow the customer to determine the potential for such a breach and guide or lead further investigation.

Breach Monitoring & Reporting

The customer will have appointed a Data Protection Officer, or other suitable senior representative, who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact, or containment. All data breaches should be reported to this person with immediate effect, whereby the procedures detailed in this policy are followed.

Breach Incident Procedures

Identification of an Incident

As soon as a data breach / suspected data breach has been identified, it should be reported to the customer DPO / representative immediately so that any existing breach procedures can be initiated and followed without delay.

Reporting incidents fully and with immediate effect is essential to the compliant functioning of the customer.

As soon as an incident has been reported, measures must be taken to contain the breach, if not already done so. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the customer prior to investigation and reporting. The measures taken are noted on the incident record in all cases.

SEE: ARO Critical Security Incident Response Plan – Customer

Breach Recording

In cases of data breaches, the Data Protection Officer or other senior customer representative is responsible for carrying out a full investigation alongside the CSIRT team, recording the incident on any established breach logs, and making any relevant and legal notifications. Wherever possible, without jeopardising containment or eradication phases, the CSIRT should aid the investigation.

If applicable, it is the responsibility of the customer DPO or other representative to notify the Supervisory Authority and ensure the data subject(s) are notified in accordance with the GDPR requirements. It is not the responsibility of ARO to make any notifications on behalf of the customer.

Breach Risk Assessment

The customer Data Protection Officer or other senior representative will need to conduct a risk assessment to understand their obligations in the event of a breach of personal information.

The appointed lead should keep an ongoing record detailing the nature of the incident, steps taken to preserve any evidence etc to aid in the risk assessment.

In the application of this record keeping consideration must be given to the availability of information from the customers environment, and any limitations. Such information should be communicated to the customer DPO / representative as soon as possible to aid in their decision-making process.

NB: Although we can provide information regarding the facts of the incident as they are known, the ultimate risk assessment and decision making process must remain the responsibility of the customer.

Breach Notifications

If applicable, it is the responsibility of the customer DPO or other representative to notify the Supervisory Authority and ensure the data subject(s) are notified in accordance with the GDPR requirements. It is not the responsibility of ARO to make any notifications on behalf of the customer.

Responsibilities

ARO will ensure that all staff are provided with the time, resources, and support to learn, understand, and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines in conjunction with the Critical Security Incident Response Procedure – Customer.

The customer Data Protection Office / senior representative is responsible for compliance review and gap analysis monitoring and the subsequent reviews and action follow ups.