Data Breach & Information Security Policy

Version: Data Breach & Information Security Policy V2026_v2.Docx
Last Reviewed: 5 November 2026
Next Review: 1 December 2026

Certificate No:359292021

Certificate No:460492024

Contents

1 Introduction 3
2 Purpose 3
3 Scope 3
4 Definition / types of incident 4
5 Reporting an information security event, incident or data breach 5
6 Assessment and classification of information security events 5
7 Containment and recovery 6
8 Investigation and risk assessment 6
9 Notification and escalation 7
10 Evaluation, lessons learned and closure 8
11 Allegations of personal data breach by a third party 8
12 Appendix I 9
12.1 Data breach report form 9
13 Appendix II – Contact details 10

1 Introduction

Acuity holds, processes and shares personal, confidential and commercially sensitive information and relies on information systems to support the delivery of its services. This information and the systems used to process it are valuable assets that must be appropriately protected.

Acuity takes appropriate measures to protect information against accidental or deliberate loss, unauthorised access, disclosure, alteration, destruction or disruption.

A compromise to the confidentiality, integrity or availability of information or information systems may result in harm to individuals, disruption to Acuity's operations, reputational damage, contractual or legislative non-compliance and/or financial loss.

2 Purpose

Acuity is required to maintain appropriate arrangements for protecting personal and other confidential information and for managing information security events, information security incidents and personal data breaches.

This Policy sets out the procedures to ensure a consistent and effective approach to the identification, reporting, assessment, investigation, response, escalation, recording and review of data breaches and information security incidents across Acuity.

The Policy supports Acuity's obligations under applicable data protection legislation and its Information Security Management System, including the requirements of ISO/IEC 27001.

3 Scope

This Policy applies to all information, information assets and information systems used by or on behalf of Acuity, regardless of format or location. This includes personal data, client and respondent information, commercially sensitive information, electronic systems, devices, applications, networks and physical records.

This Policy applies to all Acuity staff and associates. This includes workers, temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of Acuity.

The objective of this Policy is to ensure that information security events and incidents are reported and assessed appropriately, incidents are contained and investigated, risks and impacts are minimised, appropriate notification and corrective action takes place, and lessons are used to prevent recurrence.

Failure to comply with Acuity's data protection and information security policies and procedures may, where appropriate, result in disciplinary, contractual or other appropriate action.

4 Definition / types of incident

4.1 Information Security Event

Information Security Event: An identified occurrence relating to Acuity's information, information systems or security controls that may indicate a potential security issue. Information security events will be assessed to determine whether they should be classified as information security incidents.

4.2 Information Security Incident

Information Security Incident: An event that has resulted in, or could result in, the compromise of the confidentiality, integrity or availability of Acuity's information or information systems. This may include phishing, malware, unauthorised access, compromised accounts, lost or stolen devices, inappropriate information sharing, security vulnerabilities and supplier-related security incidents. An information security incident does not necessarily constitute a personal data breach.

4.3 Personal Data Breach

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

An information security event or incident may include, but is not limited to:

- Loss or theft of confidential information or equipment;
- Phishing or other suspicious communications;
- Malware or ransomware;
- Compromised user accounts or credentials;
- Unauthorised access to information or systems;
- Actual or attempted cyberattacks;
- Accidental or unauthorised disclosure of confidential or personal information;
- Incorrect access permissions or inappropriate information sharing;
- Loss, alteration, corruption or unauthorised deletion of information;
- Security vulnerabilities;
- Significant system or equipment failure affecting the security or availability of information;
- Supplier-related information security incidents;
- Human error affecting information security;
- Physical events such as fire or flood affecting information or systems.

5 Reporting an information security event, incident or data breach

Any individual who accesses, uses or manages Acuity's information is responsible for reporting any actual or suspected information security event, information security incident or personal data breach without undue delay to the Data Protection Officer and/or Director responsible for IT, as appropriate (see Appendix II below for current names and contact details of all key roles).

Individuals must report suspected events even where they are uncertain whether an information security incident or personal data breach has occurred. The subsequent assessment and classification will be undertaken by the appropriate responsible person.

If an event or incident occurs or is discovered outside normal working hours, it must be reported as soon as practicable.

The initial report should contain, where known, full and accurate details of the incident, when it occurred (dates and times), who is reporting it, the systems or information potentially affected, whether personal data may be involved and any immediate containment action taken.

Information security incidents and personal data breaches will be recorded within Acuity's **Data Breach & Information Security Incident Register in SmartSuite**. An Incident Report Form should be completed as part of the reporting process. (See Appendix I).

6 Assessment and Classification of Information Security Events

All reported or identified information security events will be assessed by the Data Protection Officer and/or Director responsible for IT, as appropriate, to determine whether they should be classified as information security incidents.

The assessment will consider:

- the type, frequency and volume of the event or related events;
- the information and systems affected;
- whether unauthorised access, disclosure, alteration, loss or disruption has occurred or may have occurred;
- the sensitivity and importance of the information affected;
- the effectiveness of existing security controls;
- the actual or potential impact on the confidentiality, integrity or availability of information;

- the impact on Acuity's operations, clients or other interested parties; and
- whether similar or repeated events indicate a wider security issue.

The outcome of the assessment will determine whether the event requires no further action, continued monitoring, or classification and management as an information security incident.

Where an information security incident involves personal data, it will additionally be assessed to determine whether it constitutes a personal data breach and whether regulatory, contractual or other notification requirements apply.

Assessment and classification decisions will be recorded where appropriate within the Data Breach & Information Security Incident Register and associated Incident Report Form.

7 Containment and recovery

The DPO and/or Director responsible for IT, as appropriate, will determine whether the incident is continuing and whether immediate containment action is required. Appropriate steps will be taken without undue delay to minimise its impact and prevent further compromise.

Following the assessment and classification described in section 6, the DPO/Director for IT in liaison with relevant officers to establish the severity of the incident and who will take the lead investigating the incident (this will depend on the nature of the incident in some cases it could be the DPO).

The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the incident could cause.

The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

Advice from experts may be sought in resolving the incident promptly.

The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

Immediate actions may include securing or disabling accounts, changing credentials, isolating affected devices or systems, restricting access, preserving relevant evidence, contacting relevant system or IT suppliers and taking appropriate steps to maintain or restore normal business operations.

8 Investigation and risk assessment

An investigation will be undertaken by the LIO immediately and wherever possible within 24 hours of the incident being discovered / reported.

The LIO will investigate the incident and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- type and nature of the event/incident;
- systems and information affected;
- type and sensitivity of information;
- confidentiality, integrity and availability impacts;
- whether unauthorised access occurred;
- whether information was disclosed, lost, altered or destroyed;
- existing protections such as encryption, MFA and access controls;
- impact on Acuity's operations;
- impact on clients, respondents or other interested parties;
- whether personal data is involved;
- number/type of individuals affected where applicable;
- actual or potential financial/contractual consequences;
- whether similar events have previously occurred;
- potential root cause; and
- whether further containment, recovery or corrective action is required.

9 Notification and escalation

The LIO and / or the DPO, in consultation with the Director(s) responsible for IT and other senior management where appropriate, will determine who needs to be notified of the incident.

Every incident will be assessed on a case-by-case basis; however, the following will need to be considered:

- Whether there are any legal/contractual notification requirements;
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- Where a personal data breach has occurred, whether notification to the Information Commissioner's Office (ICO) is required in accordance with applicable data protection legislation and ICO guidance. Where notification is required, this will be made within the applicable statutory timeframe. Guidance on when and how to notify ICO is available from their website at: https://ico.org.uk/for-organisations/report-a-breach/ *(accessed 04/11/2026)*

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific

and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with contact details for use of gaining further information or to ask questions on what has occurred.

The LIO and or the DPO must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

All actions will be recorded by the DPO.

10 Evaluation, lessons learned and closure

Following containment and resolution of an information security incident or personal data breach, the DPO and/or Director responsible for IT will review the incident, where appropriate, to determine:

- the root cause;
- the effectiveness of the response and containment;
- whether existing controls operated as intended;
- whether corrective or preventative action is required;
- whether policies, procedures, technical controls or training need to change;
- whether related risks or the Risk Register require updating; and
- whether lessons learned should be communicated to relevant personnel.

Actions arising from the review will be recorded and monitored through to completion.

The incident will be formally closed once appropriate investigation, response and corrective actions have been completed or appropriately assigned.

11 Allegations of personal data breach by a third party

It is possible a data breach allegation could be made by a third party (e.g. a tenant). If so, details of the person making the allegation and full details of the circumstances surrounding what they perceive to be the breach should be noted.

The issue should be fully investigated in line with Acuity's Data Breach & Information Security Policy. If a breach is identified, steps outlined in this policy should be followed. If no breach is identified, a formal reply should be provided to the complainant explaining why a data breach has *not* occurred. Depending upon the circumstances associated with the reporting of the allegation, the formal reply may be made directly from Acuity or, if appropriate, from a third party (for example, in instances where a tenant makes an allegation to a landlord, and the landlord is corresponding with the tenant). Copies of all correspondence should be kept on the Data Protection section of the file system.

12 Appendix I

12.1 Data Breach & Information Security Incident Report Form

To be completed by the person reporting the incident.

Please act promptly to report any data breach/information security incident. If you discover a data breach/information security incident, please notify a Director immediately, complete this form and email it to the Data Protection Officer and the Director responsible for IT.

Incident classification	e.g. Information security event, information security incident, personal data breach, information security incident & personal data breach
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information/systems affected:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For completion by the DPO and/or Director responsible for IT, as appropriate. Notification/escalation: ICO/Client/Cyber Insurer /IT/System supplier, Police, other, No external notification required	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

13 Appendix II – Contact details

Data Protection Officer

Colin Slocombe

colin.slocombe@arap.co.uk

Director responsible for IT

Jason Thompson-Graham

jason.thompson-graham@arap.co.uk