Nexus 360

Incident Policy

Staff Group to whom it applies:	All employees, contractors, consultants and third parties acting on behalf of Nexus 360.
How to access the document:	Nexus 360 computer systems.
Issue date:	June 2026
Version:	1.0
Date of next review:	June 2027
Developed by:	Danielle Cocksedge – Data Protection and Governance Manager – ARC Management and Consultancy Services
Approved by:	Mark Shevill – Director
Amendments/Updates: **Version 1.0**	New policy created for Business need.

1. Policy Statement

Nexus 360 is committed to the effective reporting, management, investigation and resolution of incidents to ensure the protection of individuals, client data, information assets, systems, services and the organisation's reputation.

As a provider of CRM solutions, automation platforms, digital business card technologies, marketing systems and consultancy services, Nexus 360 recognises the importance of identifying and responding to incidents promptly and consistently.

This policy establishes the framework for identifying, reporting, recording, investigating, managing and learning from incidents in accordance with applicable legal, regulatory and contractual obligations.

This policy supports compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Computer Misuse Act 1990
- Human Rights Act 1998
- Health and Safety at Work etc. Act 1974 (where applicable)
- Information Commissioner's Office (ICO) guidance
- Cyber Essentials requirements and recognised cyber security standards
- Applicable contractual, client and regulatory obligations

Nexus 360 is committed to maintaining a culture of transparency, accountability, continual improvement and organisational learning.

This policy should be read alongside the Nexus 360 Data Protection and UK GDPR Policy, Information Security Policy, Records Management Policy, Business Continuity Plan, Privacy Notice and other supporting governance documentation.

2. Purpose

The purpose of this policy is to establish a structured and consistent approach to incident management throughout Nexus 360.

The objectives of this policy are to:

- Ensure incidents are reported promptly and managed effectively
- Protect clients, employees, suppliers and other stakeholders from harm
- Minimise disruption to business operations and service delivery
- Protect information assets and organisational reputation
- Ensure compliance with legal, contractual and regulatory obligations
- Support timely escalation and decision-making
- Promote organisational learning and continuous improvement

- Maintain accurate incident records for governance, audit and compliance purposes

3. Scope

This policy applies to:

- Directors
- Employees
- Contractors
- Consultants
- Temporary staff
- Agency workers
- Third-party suppliers
- Sub-processors
- Anyone acting on behalf of Nexus 360

This policy applies to all incidents involving:

- Information security
- Personal data
- CRM platforms
- Automation systems
- Marketing platforms
- Digital business card solutions
- Client portals
- Cloud services
- Physical assets
- Employees and contractors
- Clients and suppliers
- Business operations and service delivery

The policy applies regardless of whether the incident occurs:

- On company premises
- At client sites
- During remote working activities
- Within cloud-based environments
- Through third-party service providers
- Through mobile devices or business applications

4. Definition of an Incident

An incident is any event or circumstance that has resulted in, or has the potential to result in:

- Harm, injury or risk to an individual
- Breach of legal, contractual or regulatory obligations
- Loss, theft or damage to organisational assets
- Service disruption or business interruption
- Financial loss
- Reputational damage
- Breach of confidentiality

- Information security compromise
- Personal data breach
- Cyber security compromise

A serious incident is one requiring immediate escalation due to its severity, sensitivity, legal obligations, financial impact or risk to individuals or the organisation.

5. Examples of Incidents

Examples include, but are not limited to:

- Personal data breaches
- Unauthorised access to systems or information
- Phishing attacks
- Malware or ransomware incidents
- Loss or theft of devices
- CRM platform security incidents
- Accidental disclosure of confidential information
- System outages affecting clients or services
- Website compromise
- Cloud service failures
- Supplier-related security incidents
- Physical security breaches
- Fraud or suspected fraud
- Health and safety incidents
- Business continuity incidents
- Significant client complaints indicating service failures

This list is not exhaustive.

6. Roles and Responsibilities

6.1 Director

The Director retains overall accountability for incident management.

Responsibilities include:

- Ensuring effective incident management arrangements are in place
- Receiving escalation of significant incidents
- Approving corrective actions where required
- Ensuring appropriate regulatory notifications are made
- Monitoring organisational risks arising from incidents

6.2 Outsourced Data Protection Officer (DPO)

The Outsourced Data Protection Officer provides independent advice and oversight relating to incidents involving personal information.

Responsibilities include:

- Advising on UK GDPR and Data Protection Act compliance
- Supporting personal data breach assessments
- Advising on ICO notification requirements and notifications
- Supporting incident investigations where personal information is involved

- Reviewing incident trends and compliance risks

6.3 Employees, Contractors and Authorised Users

All personnel must:

- Report incidents promptly and accurately
- Take reasonable steps to reduce immediate risks where safe to do so
- Preserve evidence where appropriate
- Cooperate with investigations
- Follow incident management procedures
- Escalate concerns immediately where serious risks exist

Failure to report incidents may be treated as a disciplinary matter.

7. Incident Reporting Procedure

Reporting incidents is mandatory for all personnel.

Step 1 – Immediate Response

Where appropriate:

- Protect individuals from harm
- Secure systems or information
- Contain the incident where possible
- Seek emergency assistance if required

Step 2 – Notification

Incidents must be reported immediately to a Director.

Serious incidents must be escalated without delay.

Step 3 – Recording

The incident shall be documented using the Nexus 360 Incident Report Form.

Records should include:

- Date and time
- Nature of incident
- Systems, services or individuals affected
- Immediate actions taken
- Potential risks identified

Step 4 – Risk Assessment

An assessment shall consider:

- Severity of impact
- Likelihood of recurrence
- Regulatory implications
- Client impact
- Information security implications

An overall risk rating shall be assigned:

- Low
- Moderate
- Significant
- Serious

Step 5 – Investigation and Resolution

Incidents shall be reviewed and investigated proportionately according to risk and impact.

Corrective and preventative actions shall be identified where appropriate.

8. Risk Ratings and Response

Low Risk

- Minimal impact
- Localised issue
- Managed through routine corrective action

Moderate Risk

- Investigation required
- Corrective actions documented
- Monitoring required

Significant Incident

- Formal investigation required
- Director involvement required
- Root cause analysis completed
- Action plan documented

Serious Incident

- Immediate escalation to Director
- Urgent containment measures implemented
- Regulatory reporting considered
- Formal investigation undertaken
- Senior management oversight required

9. Information Security and Personal Data Breaches

All actual, suspected or potential personal data breaches and information security incidents must be reported immediately to a Director and the Data Protection Officer.

Examples include:

- Unauthorised access to personal information
- Accidental disclosure of client information
- Lost or stolen devices
- Phishing attacks
- Ransomware incidents

- Misdirected emails
- CRM security incidents
- Unauthorised account access

Where a personal data breach occurs, Nexus 360 shall:

- Assess risks to individuals without undue delay
- Record the breach within the incident register
- Implement containment measures
- Investigate root causes
- Implement corrective actions

Where required, the Information Commissioner's Office shall be notified without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Affected individuals shall be informed where legally required.

10. Incident Recording, Monitoring and Learning

All incidents shall be:

- Recorded within a central incident register
- Reviewed for trends and recurring issues
- Subject to root cause analysis where appropriate
- Used to identify corrective and preventative actions
- Reported to management where necessary

Nexus 360 adopts a lessons-learned approach to incident management and continual improvement.

11. Confidentiality and Record Keeping

Incident records shall:

- Be stored securely
- Be protected from unauthorised access
- Be managed in accordance with UK GDPR requirements
- Be retained in accordance with organisational retention schedules
- Be available for audit, compliance and regulatory purposes where required

Access shall be restricted to authorised personnel with a legitimate business need.

12. Non-Compliance

Failure to comply with this policy may result in:

- Corrective action
- Removal of system access
- Disciplinary action
- Contract termination
- Legal or regulatory action where appropriate

13. Related Policies and Documents

This policy should be read alongside:

- Data Protection and UK GDPR Policy
- Information Security Policy
- Records Management Policy
- Privacy Notice
- Business Continuity Plan
- Cyber Security Procedures
- Supplier Management Procedures
- Confidentiality Agreements

Appendix 1

Nexus 360 - Incident Report Form

Name of Person Completing This Form: _____

Date of Report: _____

Date and Time of Incident: _____

Type of Incident (Select One):

□ Information Security

□ Data Protection

□ Cyber Security

□ System Failure

□ Client Service Issue

□ Health and Safety

□ Physical Security

□ Fraud

□ Business Continuity

□ Other

Client(s) Involved (if applicable): _____

Employee(s) Involved (if applicable): _____

Location of Incident: _____

Who Has This Been Reported To? _____

What Happened?

(Provide a factual account in chronological order)

_____
_____
_____
_____

Risk Assessment

Severity of Impact: _____

Likelihood of Recurrence: _____

Overall Risk Rating: Low / Moderate / Significant / Serious

Why Did This Happen?

_____
_____
_____
_____

Actions Already Taken

_____
_____
_____
_____

Further Actions Required to Prevent Recurrence

_____
_____
_____
_____

Submit Completed Form to: Director / Data Protection Officer

Appendix 2

Risk Assessment and further action

	CONSEQUENCE SCORE				
LIKELIHOOD SCORE	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
1 Rare	1	2	3	4	5
2 Unlikely	2	4	6	8	10
3 Possible	3	6	9	12	15
4 Likely	4	8	12	16	20
5 Certain	5	10	15	20	25

INCIDENT SCORE (Consequence Score X Likelihood Score)		
1-3	Low	May require no further action, or minimal investigation to ensure all details are correctly collated
4-8	Moderate	Requires full investigation and a review of possible outcomes/actions
9-14	Significant Event	Requires a full investigation, action plan and inclusion in reports to senior management and integrated governance
15-25	Potential SUI	Report to relevant authorities whilst all actions applied to Significant Event are carried out. Authorities responsible for appraising reported Potential Serious Untoward Incidents will inform the process accordingly.