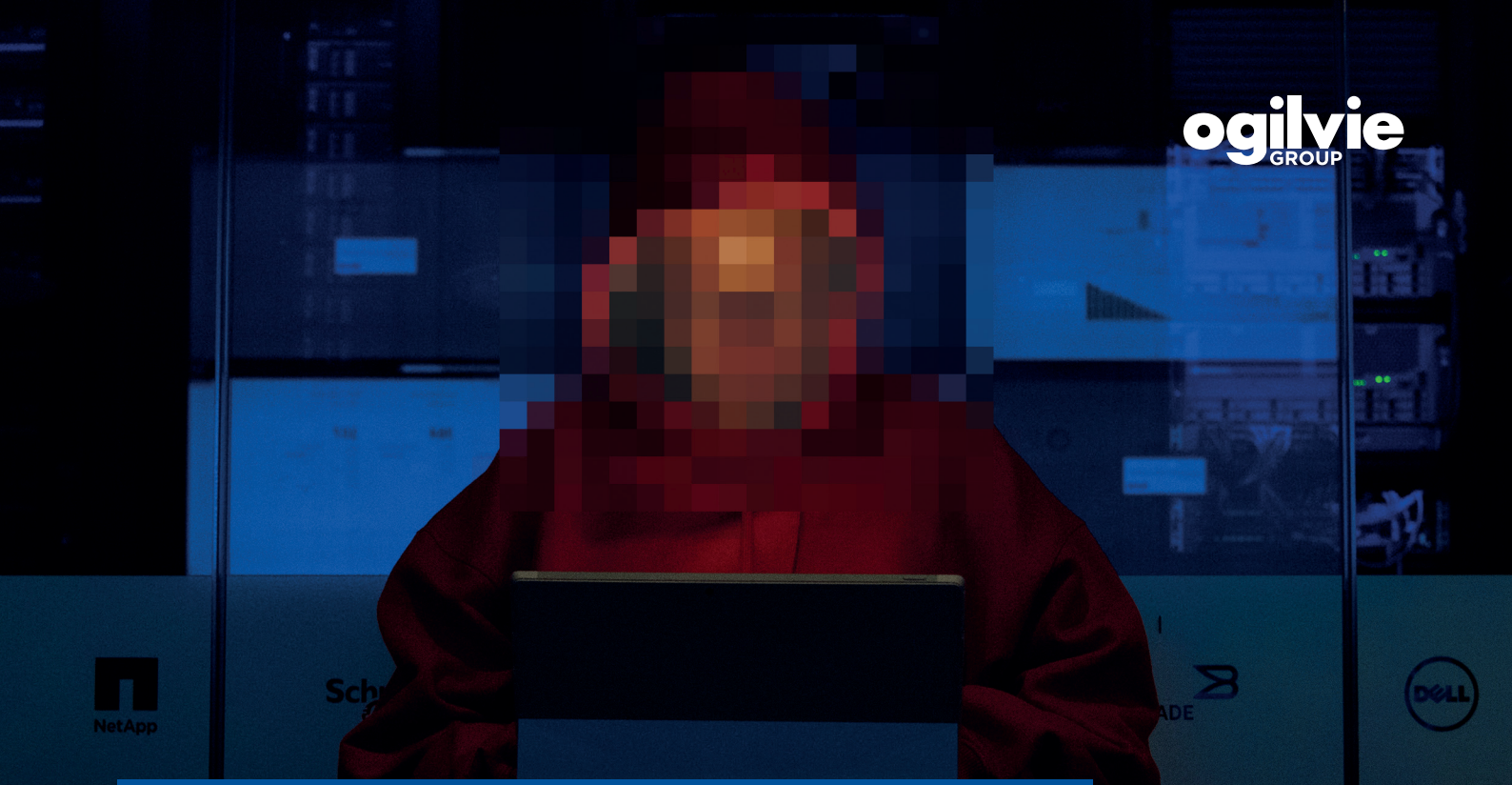

Information Security Incident Management Policy

Version 1.2

Date of issue: 12/06/2018
Last Revision: 17/08/2018

1. Overview

To ensure compliance to the data protection regulations (Data Protection Act 2018 and EU General Data Protection Regulation (GDPR) we need to effectively manage information security incidents. Potential and actual information security incidents have the ability to increase year on year if not effectively managed. These events could have both compliance and legal consequences. Therefore, OGILVIE GROUP have developed an Information Security Incident Management and Reporting Policy (and underpinning process) to ensure that a managed and consistent framework is in place to both capture and learn from such information security incidents.

This Policy addresses:

- Reporting events and weaknesses
- Managing incidents
- Collection of evidence
- Learning from an incident

The objectives of the OGILVIE GROUP Incident Management Process are:

- To establish whether a suspected incident is in fact such a security incident;
- To analyse an incident;
- To contain an incident, to eradicate the cause(s), and to recover from the incident;
- To learn from the incident, with a view to avoiding a recurrence and of its ill effects;
- To minimise any necessary OGILVIE GROUP disruption.

A security incident is defined as a breach, threat, weakness or malfunction that may have an impact upon the security of OGILVIE GROUP information related assets. Incidents include but are not limited to:

- Unauthorised disclosure of information
- Unauthorised access to information
- Unauthorised modification of information
- Unauthorised Access to premises
- Back up process failure
- Theft of an asset (hardware or information in electronic format)
- Introduction of malicious (malware, virus) software on to the OGILVIE GROUP network
- Wilful damage to an asset
- Deliberate Breaches of Security Policies e.g. Information Technology Policy and Social Media Policy.
- Events which have an impact on business continuity e.g. denial of service attacks

A security incident may be reported in a number of ways;

- An employee will inform the IT department;
- A Departmental manager may raise a concern over a member of staff;
- Excessive or inappropriate use may be identified as part of routine monitoring of web and e-mail communications;
- An incident may be identified as part of an internal or external audit.

Responsibility

All incidents must be reported to the Data Protection Representative by either email or verbal communication. Once a security incident has been identified all relevant details should be made available when reporting the incident, so that a complete investigation can be conducted.

All employees and third-party contractors who have a relationship with the organisation are directly responsible for reporting security incidents. All actual or potential incidents must be reported to:

Data Protection Representative
dataprotection@Ogilvie.co.uk

Security Incident Management Process

The Data Protection Representative will deal with incidents in strict confidence.

They Shall:

- Coordinate the investigation of the incident;
- Ensure that the extent of the incident is clearly identified;
- Raise a Security Incident Log ;
- Implement the necessary immediate corrective action (if it is within their ability);
- Escalate to the relevant member of staff as appropriate;
- Identify any preventive measures to be considered;
- Report the outcomes to the Company Board;
- Make sure that incidents are included on the agenda for the next meeting of the board at management review

1. Once an incident has been reported to the Data Protection Representative, the incident is then logged onto a security incident report log.

2. The Data Protection Representative records who raised the incident and all individuals associated with the incident (either employees or external personnel).

3. The Data Protection Representative will at this point 'classify' the incident if possible and input as much information in the log as possible surrounding the nature, type and extent of the incident.

4. The Data Protection Representative then makes decision as to who will be co-ordinating the management process for the incident; the relevant staff members will be recorded on the incident management log.

5. The incident is then dealt with and eventually **'CLOSED'**; in some cases, for significant or major incidents the Business Continuity and or Disaster Recovery Procedures may be invoked.

6. Once the incident has been **'CLOSED'**, an audit trail will be maintained including the detail of the **'CORRECTIVE'** and / or **'PREVENTATIVE'** action taken. Only the Data Protection Representative can close the incident. Closing an incident requires a closure statement.

7. An Incident Report is produced and maintained by the Data Protection Representative detailing Incidents, this will be put to the Board for review at the next Board Meeting.

2. Document Owner and Approval

The Data Protection Representative is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR.

A current version of this document is available to all members of staff on the Group Intranet.

Date	Version	Document Revision History	Document Author/Reviser
12 June 2018	1.0	Document Creation	Debra Cairns
7th August 2018	1.1	Document Review	John Watson
17th August 2018	1.2	Document Approved	John Watson

John F. Watson
Group Financial Director

17th August 2018