# Contact with Authorities and Special Interest Groups Policy

## Brunel University London

***An ISO/IEC 27001:2013:*** *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

**Mick Jenkins**
Chief Information Security Officer

# Document History

| Version | Author | Comments | Date |
|---|---|---|---|
| V 1.0 | Andrew Clarke | Initial Draft | 05/08/2019 |
| | | | |

## Document Approval

The contents of this document are confidential to Brunel University London (BUL). Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

| | |
|---|---|
| A Clarke | Mick Jenkins |
| Document Owner: Andrew Clarke | Document Approver: Mick Jenkins |
| Cyber & Information Security Manager | Chief Information Security Officer |

## Document Distribution

| Name | Title | Version | Date of Issue |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Contents

# 1. About this document

## 1.1 Purpose of Document

This purpose of this policy is to describe the Brunel University's policy on contacting Authorities and Special Interest Groups.

Please refer to Brunel University London ISMS Document University-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

## 1.2 Responsibilities

Table 1 – responsibilities

| Title / Role | Description |
|---|---|
| Relationship Owners | Are responsible for ensuring that all their Special Interest Groups (SIGs) are listed in appropriate repositories.<br><br>Are responsible for initiating and maintaining the relationship, and for ensuring that the contact information in the schedule to which this work instruction relates is current, complete and accurate. |
| Head of Security And Emergency Planning | Is responsible for ensuring that the University remains compliant with this policy in regards to contacting Authorities.<br>Is responsible for the maintenance of the Schedule for Authorities. |
| Cyber & Information Security Manager | Is responsible for writing and maintaining this policy. |

## 1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

| | |
|---|---|
| University ISMS Control Number | SOA – Number A.6– Organisation of Information Security |
| ISO 27001:2013 Conformance Control | Information Classification Objective<br>A.6.1.3 Authorities Contact<br>A.6.1.4 Special Interest Groups |

## 1.4 Scope

This policy applies to any staff that maintains a relationship with authorities or special interest groups.

## 1.5 Definitions

**1.5.1 Authorities** are organisations that require notification during an incident and will provide assistance. (e.g. Law enforcement – Met Police, Action Fraud, Regulatory bodies – Information Commissioners' Office (ICO), Financial Conduct Authority (FCA), Supervisory authorities - Environment Agency (EA), Ofsted - Office for Standards in Education, Children's Services and Skills).

**1.5.2 A Special Interest Group (SIG)** is a community of members with common scholarly interests who are interested in sharing ideas, knowledge and experiences.
The community may comprise both internal members of Brunel University and external members with a shared interest in advancing a specific area of knowledge, learning or technology where members cooperate to affect or to produce solutions within their particular field, and may communicate, meet, and organise conferences.

In a general way, you can define a special interest group as an association of individuals or organisations with interest in, or acting in a specific area of knowledge, where members cooperate / work to solve problems, produce solutions, and develop knowledge. In our case, this area of knowledge would be information security.

The 27001Academy, along with the 9001Academy, 14001Academy, and 20000Academy are examples of special interest groups. Other examples are manufacturers, specialised forums, professional associations and professional bodies, industry organisations, forums and discussion groups.

Special interest groups can assist the University's needs to keep up with business requirements and organisational risks:

- Best practices - policies, procedures, guidelines, and checklists that you can adapt to the University's needs.
- Market and security trends related to education: laws and regulations, academic, staff and organisational requirements, suppliers' situations your organisation has to be aware of or comply with.
- News and alerts about threats, vulnerabilities, attacks, and patches.
- News related to new technologies and products - improve security, or to achieve the same level with reduced costs and/or effort.
- Specialised consultancy.
- Specialised support to handle information security incidents – see Contact with Authorities (e.g., other organisations, police, government security agencies, etc.).

## 2. Contact with Authorities

Appropriate contacts with relevant authorities must be maintained and the University's legal responsibilities for contacting authorities such as the Police, the Information Commissioner's Office or other regulatory bodies are continued.

Particularly relevant to utilities, telecoms, banking organisations and the emergency services. Where attacks stem from the internet various authorities and providers may need to be called to action in order to divert /suppress / mitigate the threat.

2.1. All authorities shall be listed in REC-6.6A – Schedule for Authorities - retained in an appropriately shared and access controlled repository.

2.2. Head of Security and Emergency Planning will keep records up to date.

2.3 The REC-6.6A – Schedule for Authorities should identify which and when contact is made by the appropriate relationship owner with specific contact circumstances, and the nature of the information provided. It should clearly identify who is responsible for contacting authorities (e.g. law enforcement, regulatory bodies, supervisory authorities), which authorities should be contacted (e.g. which region/country), and in what cases this needs to happen.

2.4 Specification of the manner and timing in which breaches shall be communicated to external authorities so as to ensure appropriate reporting.

2.5. The Gold Incident Management Team (Gold-IMT) shall have version controlled copies of REC-6.6A with their personal copies of the business continuity plan.

## 3. Contact with Special Interest Groups (SIGs)

Appropriate contacts with special interest groups or other specialist security forums and professional associations must be maintained.

Some of these issues may be available for free (accessing public content on the Internet, signing up for a regular newsletter, or identifying the person / job title to be in contact with a professional association or state agency), and some may require payment (consultant or support services).

However, in the latter case it is recommended to establish contact with potential suppliers through the procurement process (it is always better to have a previous relationship than to call only in an emergency) and identify this as a Key Supplier rather than a SIG.

3.1. Relationship owners will keep appropriate contacts with Special Interest Groups (SIGs) or other specialist security forums and professional associations maintained.

3.2 Contact details, business cards, membership certificates, diaries of meetings etc. can provide evidence of professional contacts, particularly for information risk, security and compliance specialists. Valid contact details embedded within incident response, business continuity and disaster recovery plans provide further evidence of this control, along with notes or reports from previous incidents concerning the contacts made.

3.3 In the cases where you have to send or receive information, be sure to verify whether there is an agreement about how the shared information will be protected. (Ref Information Classification Policy and Encryption Policy).

3.4 When using a Special Interest Group, be cautious with the information provided.

- The quality of the information provided: Not all of them have precise or updated information (some only repost news or information from other sources).
- The availability of the information: what is the update frequency of the information? If the source you use takes too much time to update the information, the University could be exposed to a problem or risk for a longer period.
- The legitimacy of the source: Not all Special Interest Groups are authorised representatives of the one responsible for the information (e.g., manufacturers have specific forums to communicate with their clients or to provide patches). Another case is if security peers recognise the group as a reliable source of information.