Document Control Information

NB: If you are reading this as a printed document you are requested to check the online **Controlled Documents Master List** to ensure that it is the latest version before following the guidance it contains. If you discover this version is out of date, please destroy it and use the latest version.

Document Details	
Document Name	Information Security Statement
Purpose of Document	To describe the high-level approach to the management of information security at BCS, The Chartered Institute of IT
Document Number	STA 003
Document Version Number	V3.5
Document Status	Approved
Document Owner	Group CEO
Data Classification	Private
Security Category	Low
Prepared by	Director of Business Technology
Date Approved	September 2014
Effective Start Date	September 2014
Effective End Date	
Approved by	Executive Board
Next Scheduled Review	**July 2020**

Version History			
Version Number	**Date Amended**	**Changes Made**	**Checked by**
V3.5	03/07/19	Reviewed - no changes	K Zoldak
V3.5	17/04/18	Simplified some wording	C Harris
V3.4	04/01/17	Reviewed – no changes	C Harris P Fletcher J Buttriss
V3.3	01/10/16	Updated in light of feedback from BSI Stage One audit, URM consultant and CEOs	R Levermore P Fletcher and J Buttriss
V3.2	19/08/15	Reviewed – no changes	Katrina Zoldak
V3.1	09/09/14	Approved revisions following annual review.	Carl Harris

Distribution List	
Name	**Title**
Paul Fletcher	BCS Group CEO
	All staff via the Green Room
	Member Groups Officers via the BCS website

BCS, The Chartered Institute for IT

Information Security Statement

July 2019

Information Security

In this day and age, it is increasingly important that we are concerned with Information Security. The information that we hold and process within BCS is sensitive in nature. The loss or disclosure of the data could lead to prosecution or serious harm to our reputation. There is also a risk to the privacy of our members, our customers and the organisations with whom we work.

Because of these risks, BCS takes very seriously the need for Information Security and we have implemented systems and processes, which are aligned with the International Standard (ISO27001), to define the way that we manage it.

All new members of staff will receive awareness training as part of the induction process and existing staff will all receive awareness training at regular intervals. Our volunteers, partner organisations and contractors will also be required to observe the standard in their dealings with us, or with others on our behalf. If you are unsure about any of the guidance contained in this statement or would like further information, it is your responsibility to contact your manager to ask for assistance. Similarly, if you have an idea about how to improve our systems or processes, please let them know.

It is the responsibility of every member of staff of the organisation, including myself, to become familiar with our systems and processes and comply with the policies and procedures defined within them. We take this requirement most seriously – failure to comply with our policies and procedures could lead to disciplinary proceedings. We will review how well we as an organisation comply with the systems and processes we have defined and find new ways to improve how we manage Information Security.

The Executive Team fully support our approach to Information Security Management and require all members of staff, volunteers, partner organisations and contractors to do the same.

Any deviations from this Statement must be authorised by Executive team.

Paul Fletcher
Group Chief Executive
BCS, The Chartered Institute for IT

Information Security Statement

The aim of this Information Security Statement ("this Statement") is to set out the actions and measures required to protect information from security threats. Compliance with this Statement protects BCS' information and minimises the effect of a security incident.

Information may be in paper or electronic format, held on BCS computer systems or removable storage devices, spoken over the telephone or in documents sent by post or courier. This Statement refers to all such information as BCS Information and the systems on which it is held as BCS Information Systems.

It is a requirement that:

- Information, data and information processing facilities shall be protected against unauthorised access.
- Information shall be protected from unauthorised disclosure
- Confidentiality of information assets shall be a high priority
- Integrity of information shall be maintained
- BCS requirements, as identified by information owners, for the availability of information assets and information processing facilities required for operational activities shall be met
- Statutory, and expressed and implied legal obligations shall be met
- Regulatory, contractual and compliance obligations shall be met
- Requirements for the continuity of information security shall be determined and maintained within BCS' business continuity arrangements
- Unauthorised use of information assets and information processing facilities shall be prohibited; the use of obscene, racist or otherwise offensive statements shall be dealt with in accordance with other policies published by BCS
- This statement shall be communicated to all staff for whom information security training shall be given.
- A systematic approach to information security risk management shall be followed and shall be a dynamic and continual process
- Information security shall be managed through a formal Information Security Management System (ISMS) that shall be defined within a documented framework
- The ISMS shall be continually improved through a process of performance evaluation that includes monitoring and measurement against defined objectives, internal audit and management reviews
- All breaches of information security, actual or suspected, shall be reported and investigated in line with BCS' published policies
- Controls shall be commensurate with the risks faced by BCS.

In support of this statement, more detailed operational security policies and procedures shall be developed for staff, information assets and information processing facilities. These policies shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

BCS Information may contain BCS' intellectual property and confidential information, the personal information of staff, customers and members all of which must be held securely at all times to safeguard BCS' business continuity, reputation and interests and the interests of all those having an interest in BCS Information.

All those with access to BCS information are responsible for complying with this Statement.

All BCS managers are directly responsible for day to day management of this Statement and for implementing this within their business areas and for ensuring compliance by their staff.