Supplier Policy

V2.7 April 2025

CONTENTS

This document forms part of our Management Systems and compliance is mandatory for all staff and contractors. If you find any weaknesses in the document or examples of non-compliance, please report it to the Compliance Team at compliance@bcs.uk.

1 Policy Statement

BCS seeks to conduct our relationships with our suppliers in a suitable and proper way, and we seek to develop relationships with suppliers that conduct their business in a legal and ethical manner. Our supplier principles apply to all companies, suppliers and manufacturers that we conduct business with.

We aim to protect BCS assets, and data subject's personal information that is accessible by third parties, and to ensure fair and consistent practice in our dealings with suppliers. BCS accepts that it has the legal responsibility for protecting information including its suppliers' information. BCS is committed to using providers with very high reliability for its services to members, learners and other categories of customers.

This policy sets out the standards that BCS expects its suppliers to comply with as well as dealing with the approval and monitoring of our suppliers. BCS expects suppliers to have suitably trained staff, subcontractors and agents to a level appropriate to comply with this policy, relevant laws and regulations.

This policy should be read in conjunction with the Ethical Business Policy.

2 Relationship with Suppliers

2.1 BCS Obligations

BCS will

- follow/ support universal human rights in compliance with the UN's conventions on human rights and UK human rights laws;
- conduct our business in accordance with applicable laws and regulations;
- seek to be honest and fair in our relationships with our suppliers;
- aim to pay suppliers and subcontractors in accordance with agreed terms;
- seek to ensure that our terms of business are explained clearly;
- not offer, pay or accept bribes or substantial favours, including hospitality and we expect the same from our suppliers;

2.2 Supplier Obligations

We expect our suppliers to:

- operate employment practices and support universal human rights in compliance with UN's conventions on human rights and UK human rights laws;
- conduct their business in accordance with applicable laws and regulations;
- provide a safe workplace with policies and practices in place to minimise the risk of accidents, injury, and exposure to health risks;
- adhere to the Modern Slavery Act;
- compensate their employees fairly and competitively relative to their industry in full compliance with applicable local and national wage and hour laws, and to offer opportunities for employees to develop their skills and capabilities;
- in the event their employees have lawfully chosen to be represented by third parties, bargain in good faith and not to retaliate against employees for their lawful participation in labour organisation activities;

- conduct business in ways that protect and preserve the environment. At a minimum, we expect our suppliers to meet applicable environmental laws, rules and regulations in their operations in the countries in which they do business;
- follow all applicable laws, and similar standards and principles in the countries in which they operate;
- present any information regarding subcontractors, production units and geographical position requested by BCS;
- protect and use BCS assets responsibly, with due care and only when and for authorised business-related purposes. BCS assets include financial assets, physical assets, technology and systems, intellectual property rights, and information about the BCS products, services, customers, systems and people;
- disclose all actual or potential conflicts of interest (e.g. personal relations of supplier management with BCS staff) due to either business or personal relationships with customers, other suppliers, business associates, or competitors of BCS, or with other BCS employees.
- compete fairly and in line with relevant anti-trust laws in the marketplace. Suppliers must therefore calculate, quote and submit price(s) and/fees contained in any bid, proposal or invoice independently without collusion, consultation, communication or agreement with any other competing supplier.
- strictly limit and safeguard the confidentiality, integrity and availability of information belonging to BCS and any third parties, including any information created, received or learned by the supplier whilst engaged for or on behalf of third parties;
- obtain the appropriate registrations and licenses from the relevant regulatory bodies prior to conducting any form of business in connection with BCS. In case Suppliers are aware that proceedings are started to limit, withdraw or otherwise alter the license, they must proactively inform their BCS contact in writing
- inform their BCS contact in writing if they, acting in good faith, reasonably believe that anybody working for or on behalf of BCS has committed an illegal or dishonest act, or an act that causes, or is likely to cause, harm to people or property or an act that is a known or suspected violation of this Policy.
- inform BCS of a data breach if it impacts BCS or its customers in a timely manner. This can be done using breachnotification@bcs.uk . See Section 7 for more information.

BCS is fully committed to the international fight against money laundering and the financing of terrorism as well as to the compliance with applicable sanction regimes. Suppliers must not engage in, support or tolerate any activity in connection with BCS which infringes or circumvents applicable laws against money laundering or terror financing, applicable sanctions or which otherwise could be interpreted as illegal activity.

3 Approval Process

It is recognised that BCS utilises the products and services of companies with widespread presence providing cloud-based services supported by large networks of worldwide distributed servers, presumed to have adequate Information Security protection and Business Continuity capabilities.

When a service is outsourced to a business partner, the management of the associated risks are also partially or totally transferred by BCS to that provider. However, the responsibility for the effective management of those risks remains always with BCS.

Therefore, BCS will ensure that all providers delivering important services for or on behalf of BCS Group must have in place effective risk management processes to ensure their operational reliability.

3.1 Risk Methodology for New Suppliers

BCS will use a simple "Replaceable / Important / Critical" weighting when assessing new suppliers:

About the Service				
Importance of Service	Replaceable		Important	Critical
Type of Personal Information	None	Basic	Special Category	Special Category
Method of Transfer	None	Encrypted	Partially Encrypted	Unencrypted
Volume of Personal Data	None	Low	Medium	High
Frequency of Transfer	None	Annually	Monthly	Daily
About the Organisation				
Previous Data Breach	None	One	Fewer than two	More than two
Locations and Transfer	None	Domestic	International – EU	International non-EU
Value of service to BCS	<£50,000 per annum		£50,000 to £100,000	>£100,000
Reputational Risk	Low Risk	Low	Medium Risk	High Risk
Score	0	1	2	3
Risk Rating	Low Risk <10	Low Risk < 10	Medium Risk 11 – 16	High Risk > 17

A score is given for each box and then they are added up to get a BCS risk rating.

All suppliers that are classified as critical must hold UCAS accredited ISO27001 and ISO22301 unless the Head of Legal & Compliance or an Executive overrules (and documents reason for) doing so.

BCS will check the ISO certificates on the supplier's website and also check that the certificates are from an UCAS accredited body either on the BSI Certified Client Directory BSI-issued certificates and verifications | BSI (bsigroup.com)/ an equivalent website. Alternatively we will ask the supplier to send us copies of the certifications.

4 Monitoring Process

All Key Suppliers will be reviewed whilst being onboarded via the Supplier review form and then annually by the business owners. Annual supplier reviews will be assessed against agreed KPIs or SLAs along with any data breaches. BCS request that as part of the review, the Annual supplier review form is completed. If the Annual supplier review form is not completed as part of the review, an appropriate internal review will be conducted by BCS Compliance.

5 Information Security

When a contract is agreed or reviewed it must be assessed to ensure that it includes the latest data protection regulations and information security requirements.

BCS will accept supplier issued contracts, but these must contain adequate data protection processing clauses and security requirements. All data processing contracts must be

checked by the Legal Team prior to being signed off. Contracts must be signed by authorised signatories of both parties.

Where relevant, suppliers will only be authorised to test data that the BCS has, but in limited circumstances, suppliers may be allowed to access live data. In these circumstances the access to the data will be monitored and contractual terms will take this into account.

Where there is a need for confidentiality of information, non-disclosure agreements must be used. If the supplier wishes to use their NDA, your BCS point of contact should be notified and this referred to our Legal team for their review and approval.

Where terms are provided but are not required to be signed, these terms will be attached to the supplier account. The BCS Legal Team must be provided with a copy in good time in order to review and approve that they are suitable for the product or service being purchased.

The Legal Team will work with any area of the business who is in discussions with suppliers, including but not limited to supplier selection, negotiating new contracts or amending existing contracts. It is recognised that existing contracts may not meet these requirements, so this will be assessed when they come up for renewal.

Any new contracts with suppliers must be referred to the Legal Team for review in good time prior to signature or acceptance of the terms, to ensure that BCS is adequately protected.

6 Auditing

Contracts should try to ensure that BCS or another party appointed by BCS has the right to audit the supplier's processes and controls as well as those of its suppliers which impact BCS where appropriate. Audits may be undertaken if there has been a breach of security or if other risks come to light which cause BCS concern.

It is accepted that in some cases we will not be able to ask suppliers to complete our due diligence process or be able to audit these organisations. In that event, the contract owner must record any incidents and review the contract/ on-line terms every three years.

In cases where suppliers are unable to complete our due diligence process, internal reviews will be conducted.

7 Notification of an Incident

Suppliers will be expected to advise BCS of a potential or actual incident as soon as they are made aware of the incident and will be expected to ensure that their staff are aware of the requirements to report an incident.

8 Compliance with this Policy

The Supplier should be provided with a copy of this Policy before the contract is signed. Suppliers are required to maintain accurate and appropriate records to demonstrate compliance with applicable laws and regulations and this Code.

Whilst Suppliers are expected to self-monitor and demonstrate their compliance with this Code, BCS may reserves the right to audit the supplier to confirm compliance. BCS shall be entitled to terminate, in whole or in part, the Agreement and any other agreement if the

Supplier fundamentally violates this policy and in line with the termination clauses in the Agreement for breach of contract.

BCS will maintain confidentiality to the extent possible and will not tolerate any retribution or retaliation taken against any individual who has, in good faith, sought advice or reported any questionable behaviour or a possible violation of this policy.

9 Monitoring and Review of this Policy

This policy is reviewed on an annual basis in line with departmental quality standards and regulatory. We will also consider any customer feedback, trends from our internal monitoring arrangements, changes in our practices, as well as changes in legislation. If you would like to feed back any views, please discuss with the owner of this document.

For further information please contact:

BCS
The Chartered Institute for IT
3 Newbridge Square
Swindon
SN1 1BY

T +44 (0)1793 417 417

www.bcs.org