THE BRITISH LAND COMPANY PLC

Supplier Information Security Standards

We strive to make our content accessible for all however if you require information in an alternative format please contact enablenetwork@britishland.com

Document ID: ISP-14
Approved by: Head of Information Security
Date Approved: August 2023
Last Review Date: June 2025
Next Review date: June 2026
Owner: Information Security
Classification: Confidential
Version: 1.7

Supplier Information Security Standards

Table of Contents

Supplier Information Security Standards

1 Introduction

These Supplier Information Security Standards form part of British Land's Information Security policies.

1.1 Requirements for Standards

Our suppliers are integral to many of the operations conducted by British Land. In order that we maintain and uphold our values to our customers, consumers, staff and the general public, we require our suppliers to meet a high level of information security standard based on their service provision. The following standards have been developed to enable you, the supplier, to work in a conformed and uniform way with us.

1.2 General Requirements

The term "supplier" throughout this document encompasses all contractors, sub-processors and agents of the supplier. You are required to procure that the applicable standards are applied throughout your supply chain.

2 Monitoring and Corrective Actions

2.1 Corrective Actions

As part of our supplier assessment process we will ask you questions that will enable us to determine which of the six engagement types (see section 3 below) you will be categorised under. Each time you submit the assessment to us you are required to provide an attestation confirming that the information provided is true and correct.

The assessment process may also require us to return the assessment to you with further information requests until a categorisation can be determined, and/or to identify and agree with you mitigative actions that you are required to take as part of the onboarding process. Any such actions must be completed within the agreed timescales. Any request to amend an action or extend an action timescale must be agreed in writing with British Land. Failure to complete the agreed actions within the required timescales may be considered a material breach of contract.

2.2 Ongoing Monitoring

All suppliers approved to work with British Land will, as part of their contractual obligations, be required to conduct an annual attestation to the standards. The standards may be updated from time to time and it is your responsibility to ensure that you are complying with the latest version, which can be accessed on the British Land website here: British Land – Information Security Supplier Standards. British Land reserve the right to conduct audits of suppliers against these information security standards at any time.

For suppliers who support critical business services, systems, and applications, you will be required to complete a formal attestation assessment. This means that 12-18 months after the initial assessment you will be automatically issued with:

- a condensed assessment covering critical business areas and/or areas with highest risk to British Land, for continuous services only; or
- if there has been a change to the services that you provide or will provide:
    - a request to provide further information on any changes to the services provided; and
    - a new assessment designating you with a revised engagement type, and the corresponding set of standards to attest to.

3 Engagement Types

Following a supplier assessment, you will be designated as falling into one of the six engagement set out below, and will be required to comply with the corresponding standards from the table in Appendix 1. Where a supplier falls into two or more engagement types, the more in-depth categorisation (and corresponding set of standards) will be used to form the assessment. The six engagement types are:

No.	Service Category	Category Description	Example services (including but not limited to):
1	**Access our Premises – No System Access**	You provide services that require physical access to our premises but do not access any systems or data	Soft services – e.g. cleaning or property maintenance
2	**Access our Premises – Systems Access**	You provide services to British Land where you are on site and are accessing our systems, such as our CCTV, WiFi or IT infrastructure	IT technical support services CCTV operation Facilities management systems Building management systems Access control Car park systems Footfall or car counting Digital display boards
3	**Remotely access our systems at our Premises**	You provide a service whereby you access our systems from a remote location only	Technical support Application development Facilities management systems CCTV operation Access control Building management systems Digital display boards Car park systems
4	**IAAS – Host our systems** (IaaS - **I**nfrastructure-**a**s-**a**-**S**ervice)	You provide services that host our applications or other systems such as our servers or in-house developed applications	Facilities management systems CCTV
5	**SAAS – Provide a managed service we operate** (SaaS - **S**oftware-**a**s-**a**-**S**ervice)	You provide services that support and enable business processes or process our data, such as reporting applications or HR systems	Facilities management systems
6	**Hold our data on supplier system**	You provide services which require you to hold and process our data (either personal or business) on your systems	Facilities management systems Communications agency services Marketing services

4 Standard Requirements

The table in Appendix 1 outlines the standards that must be followed for each engagement type. It is aligned to the ISO27002 framework.

Requirements in blue are Data Privacy specific criteria.

Appendix 1

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
0	Sub-Contractors	If any of the systems or services to British Land are supported by or maintained by a sub-contractor, they must adhere to the following standards to ensure continuity throughout the supply chain. You are responsible for ensuring British Land's standards are fully implemented and maintained. You may be required to provide evidence accordingly.		x	x	x	x	x	x
1	Organisation	Your company has a current, management approved and published Information Security and Acceptable Use Policy, that is reviewed at least annually. Policy documents are issued to all staff members to define and confirm their information security responsibilities.	Documented policies and standards are crucial elements for risk management and governance. They set the management's view of the controls required to manage information/cyber risk.	x	x	x	x	x	x
2	Roles & Responsibilities	Your company has an individual responsible for information security. Details to be provided to British Land Information Security Team. Any changes to the role, must be reported to British Land. Your staff receive regular cyber awareness training (at least annually).	Clear definition of roles and responsibilities support the implementation of the Information Security Requirements Education and awareness is important to ensure employees are aware of cyber risks and attack vectors and can help to detect or prevent attacks.	x	x	x	x	x	x
3A	Logical Access Control	Each user account will be authenticated to a single individual using a unique identifier before access is granted to any business information, application, system, device or network. The user is wholly accountable for any activities carried out. Shared accounts are not encouraged but may be used with prior written consent from British Land. A nominated individual must be accountable for the use and management of the shared account System administrator and 'super-user' privileges are limited to a small number of	Appropriate Logical Access controls helps to ensure that Information Assets are protected from inappropriate usage		x	x	x	x	x

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
		appropriate, qualified and authorised individuals, and must not be used for 'every-day' activities. User accounts and access privileges are reviewed by management at least annually, to ensure the appropriate of access and governed segregation of duties.							
3B	Logical Access Control	You take appropriate information security measures on all user accounts by: - implementing a formal password policy - implementing multi-factor authentication - changing or disabling default system passwords. Access management processes are defined and include the following as a minimum: - Robust authorisation process for creating, amending and deleting accounts. - User access reviews every 6 months. - Mover controls that requires access to be amended or removed within 5 working days of move date. - Leaver controls that require all access to be removed within 24 hours of the leave date.	Appropriate Logical Access controls helps to ensure that Information Assets are protected from inappropriate usage		X	X	X	X	X

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
4A	Authentication	You must have a strong password policy that requires each user to comply with the following: - Passwords must be unique, hard to guess and different for each account or system. - Must have a password or phrase with a minimum of 12 characters (for standard users) or 16 characters (for privilege user accounts) with a range of character types (upper/lower case / number / special character). - Enforce password history policy with at least 24 previous passwords remembered. - Password lock out control set for 5 failed attempts with administrator required to reinstate the account. - Never reveal or share passwords with others. Change immediately if you believe it has been compromised.	Authentication controls help ensure that only approved users can access the information. Length of password trumps complexity however adopting 'three random words' is advisable. Use a password manager to store long and complex passwords. Refer to National Cyber Security Centre (NCSC) for further guidance.		X	X	X	X	X
4B	Authentication	Shared accounts and therefore shared passwords are not advisable. For instances where this is unavoidable you must comply with the following best practice: - Password must only be shared with the minimum number of trusted users. - Passwords must not be shared or exposed to unauthorised individuals. - Should someone within the authorised group leave or no longer require access, the password must be changed immediately. You must use Multi-Factor Authentication (MFA) with at least two factors for all systems and services. Where MFA is not possible, you must implement a strong password policy as outlined in 4A.	Authentication controls help ensure that only approved users can access the information.		X	X	X	X	X

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
5	Asset Management	You maintain a complete and accurate inventory of business-critical assets at all sites and/or locations that support services to British Land. You either maintain British Land's asset inventory or maintain your own records, as appropriate, meeting industry best practise standards. All changes must be accurately recorded within the asset inventory. The asset inventory must be reviewed at least annually and must be validated for completeness and accuracy. You must inform British Land, in advance, if assets are approaching or are already 'end of life' or 'end of service'.	**Definition** - Asset includes all hardware, software, information or data, and equipment regardless of where it is hosted. A complete and accurate inventory of Information assets is essential for ensuring appropriate controls, and preventing compromise, which may result in financial losses, loss of data, reputational damage and regulatory action.		X	X	X	X	X
6	Destruction	You ensure that information is securely destroyed using appropriate methods as directed by British Land (overwriting 3 times / degaussing / physical destruction.) This applies to both during and at the end of the contract period. You ensure that any data is either returned or destroyed as agreed with British Land, and provide an audit trail demonstrating this (certificate of destruction). Any decommissioned equipment with internal storage media or hard drives must be securely wiped and / or destroyed.	Secure destruction of information helps to ensure that British Land information cannot be recovered, preventing data breach, loss, or malicious activity. This includes flash memory, removeable media, printers, cameras etc.				X	X	X

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
7	Encryption	You ensure all Confidential Information and Personal Data is encrypted both at rest and in transit, to current industry standards (AES 128, SHA 256, RSA 2048, TLS 1.2). This includes at minimum: - portable devices including laptops, mobiles, tablets, removable media - data stores such as file shares, databases and storage buckets - transmission methods such as email, internet VPNs, wireless	Up to date and appropriate encryption protection and algorithms ensures the continued protection of British Land information			X	X	X	X
8	Backup/ Restore	You ensure that information is adequately backed up and recoverable as agreed with British Land. You ensure that the security of information is maintained throughout the process. Backups are periodically assessed by performing restore tests with the results recorded. Where there are any failures, you will ensure action is taken to resolve, then rerun the assessment until successful. All results to be recorded in the site register.	Backups are important controls to maintain continuity of the business. They store copies of our information and must be subject to the same controls and protection as other information.		X	X	X	X	X
9A	Logging & Monitoring	Systems are configured to ensure robust audit trails, for all activities are in place at all times. This includes at minimum: account usage, system usage, incident recording, any equipment “call home” features and regular system updates. These audit trails are secured to ensure their integrity is maintained and guarded against tampering.	Logging and monitoring are important controls to detect and respond to Cyber security breaches or recover and learn from Cyber events that have occurred by analysing relevant logs.		X		X	X	X

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
		Audit logs should be maintained, with a minimum of 3 months immediately available for analysis. Where logs contain sensitive data, these should be protected from unauthorised access.							
9B	Logging & Monitoring	You have a dedicated monitoring service with incident response management and logging security incidents with 24x7 coverage	Monitoring security events must be a continual process to ensure that incidents are raised and dealt with as soon as practical.					X	X
10	Time Synchronisation	System time must be synchronised using Network Time Protocol (NTP) to ensure that all logs are accurate.	If this control is not implemented properly then you may be unable to provide accurate incident management activities		X	X	X	X	X
11	Malware	You have measures in place to protect systems and networks from malicious code and malware. You implement, and maintain up-to-date, protection against malicious code and malware in line with good industry practice.	Anti-malware solutions are vital for the protection of British Land information.		X	X	X	X	X

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
12	Vulnerability Management	You will identify technical vulnerabilities and implement techniques to reduce or eliminate these appropriately as agreed with British Land, using industry best practices. You must ensure that suitable back-ups are taken before conducting any remediation activities. Out of date or out of support software must not be used. Only fully licenced and supportable software may be used, and it must not be more than 2 versions behind the current version available by the software vendor. All critical or high security incidents or vulnerabilities must be notified to British Land within 24 hours of discovery. You must inform the British Land Site Operational Manager, the Data Privacy team and the Information Security Team. Where you make a decision to accept the risk, this must be agreed in writing with British Land.	For example - applying regular OS updates and security patches / timely management of any out-of-bounds, zero-day or emergency patches / configuration changes / use of mitigating controls including active anti-virus software. If this control is not implemented, attackers could exploit vulnerabilities within systems to carry out cyber-attacks against British Land. Please upload evidence (either by comment or uploading standards attesting to the best practice) if possible.		X	X	X	X	X
13	Penetration Testing	Penetration testing or security application testing must be conducted regularly (at least annually or post significant change) and with an independent, reputable, qualified security provider with industry recognised accreditations for all supplier owned assets and applications. The supplier is responsible for arranging and conducting the penetration test on their own assets. You agree to share the scope and final report with British Land and ensure that findings are addressed in a timely manner, in line with industry best practice. All critical or high findings must be notified to British Land within 24 hours of discovery, together with the proposed remediation plan, and you must inform	If this control is not implemented, you may be unable to assess the Cyber threats you face and the appropriateness and strength of your defences. Industry accreditations: CHECK, CREST etc.					X	X

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
		the British Land Site Operational Manager, the Data Privacy team, and the Information Security Team. British Land will carry out site pen testing for British Land owned assets. It will be conducted by an independent, reputable, qualified security provider with industry recognised accreditations.							
14	Secure Collaboration Policy	The Business Data or Document Owner is accountable for who should have access and the type of access a user may have, both inside and outside of British Land and its suppliers. You are responsible for ensuring the data integrity is maintained. If you consider or are made aware of a data breach which may impact British Land, you must inform the British Land Data Privacy Team immediately, or within no more than 24 hours.			X	X	X	X	X

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
15	Network Security	You must ensure that all IT systems operated by you or a sub-contractor are protected from network threats. Network integrity mechanisms must cover the following: - Maintain an updated and accurate Network Architecture Diagram defining the networks boundaries. - Protect networks through defence in depth principles. - Implement network intrusion prevention techniques to detect and protect against malicious traffic. - Use strong network firewall capabilities and securely harden network devices to protect against malicious attacks. - Deny communication over unauthorised TCP or UDP ports, scanning regularly from outside the trusted network to detect authorised connections. - Review all firewall rules at least annually (internal & external), and, identify and confirm the necessary ports for you and third parties systems and software used onsite, minimising the requirement for 'Any' rules on the firewall. - Ensure all wireless access to the network is subject to authorisation, authentication and encryption protocols. - Systems must be up to date with supported licenced software with is regularly patched.			X	X	X	X	X
16	Denial of Service (DoS)	You maintain a capability to detect and protect against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. You must ensure that internet connected or externally facing channels support services to British Land have adequate DoS/DDoS protections to ensure availability of the service.	This will prevent denial of service attacks from achieving their objectives					X	X

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
17A	Remote Connection	When connecting to British Land sites remotely, you must ensure User Authentication by enabling Multi-factor Authentication and using secure, complex passwords and either: - Conditional access protocols - ensure all connecting devices have the minimum security requirements, OR - Demilitarised Zone (DMZ) - external connections should be received on a segregated network (not internal) with only specific resourced allowed to be accessed. You must perform reconciliation of all remote users at least quarterly and provide attestation to British Land upon request. You must deactivate authentication credentials within 24 hours upon notification that access is no longer required. Where British Land is providing remote access, you must provide notification with 24 hours upon notification that access is no longer required and we will deactivate the authentication credentials. You must ensure that all remote connections are configured securely, including at minimum current OS version, updated endpoint protection, latest security patches, latest anti-virus protection.	Remote access controls help to ensure only authorised and secure devices are connected to the British Land environment remotely			X		X	X
17B	Remote Connection	Access to your network must be via a secure token, provided by you. This may be physical or digital. Access to the British Land network must be via a secure token provided by British Land. You must maintain an accurate inventory of all secure tokens provided by you and/or British Land and implement a management process for conducting	Remote access controls help to ensure only authorised and secure devices are connected to the British Land environment remotely						

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
		regular reviews (at least quarterly) and monitoring of the allocation, use and return of secure tokens.							
18	System acquisition, development, and maintenance	You have an established Secure Development framework, aligned to industry best practice, to prevent security breaches and to identify and remediate vulnerabilities in the code during the development process. All applications must be tested and validated against the appropriate standards prior to release (e.g. OWASP Secure Coding)	Controls protecting application development help ensure that applications are secured at deployment.				X	X	X
19A	Incident Management	You have a documented, published and communicated incident management process which must be followed in the event of a security incident and / or data breach. You must inform British Land within 24 hours of discovery of any security incident or data breach, with the potential to impact or effect British Land operations. You must provide reasonable assistance to British Land in accordance with any agreements or obligations. You must disclose to British Land any security incidents or personal data breaches within the last 3 years, that involved the actual loss or breach of information or system compromise, whether or not resulting in financial, operational or reputational losses, regulatory or civil action. This must be disclosed to the British Land Information Security and Data Privacy teams.	An incident management and response process help to ensure that incidents are quickly contained and prevented from escalating.	X	X	X	X	X	X

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
		You have a documented, published and communicated Business Continuity Management plan that includes services being provided to British Land.							
19B	Incident Management	You formally record all incidents in an incident log, the details for which can be shared with British Land upon request (if appropriate). If the incident relates to British Land data, system or service and is either a critical or high vulnerability, you must notify British Land within 24 hours of discovery. You must inform the British Land Operational Site Manager, the Data Privacy and Information Security teams. The Business Owner is responsible for the external contract and must check to confirm the contract terms are appropriate in respect to information security.	An incident management and response process help to ensure that incidents are quickly contained and prevented from escalating	X	X	X	X	X	X

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
20	Records of Processing	Your company maintains accurate Records of Processing (RoP). Your company can provide this information to British Land on request. If the system is supported or maintained by your appointed sub-contractor, they must adhere to these standards to ensure supply chain security.	Under article 30 of the GDPR and Chapter 4 (60) of the Data Protection Act 2018, the maintenance of this information will act as evidence that you are meeting your data privacy obligations. At a minimum, as a data processor you must maintain a centralised record that captures the following information: Name and contact details of the data controller Name and contact details of the controller's representative The categories of personal data (e.g., Personal ID Data) Geographical locations to which personal data is transferred Associated contracts entered with sub processors A description of how your organisation keeps each subset of personal data secure.				x	x	x
21	Data Privacy Training	Your company provides data privacy training to all employees on induction with annual refresher training. If the system is supported or maintained by your appointed sub-contractor, they must adhere to these standards to ensure supply chain security and ensure they carry out the data privacy training.	Education and awareness is important to ensure employees are aware of data privacy legislation and their data protection obligations.	x	x	x	x	x	x

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
22	Data Transfers	Your company will not appoint a sub-processor without the prior written consent of British Land. You ensure the same Data Protection clauses (or those deemed equivalent) are in place with all sub-processors used. You keep a register of all Data Transfers which include British Land data. You keep a register of the geographical locations to which British Land data is transferred. Where personal data is transferred to locations which are not recognised as providing an adequate level of data protection, you will assist British Land in determining the impact of local surveillance laws and practices to determine the correct transfer mechanism. If the system is supported or maintained by your appointed sub-contractor, they must adhere to these standards to ensure supply chain security	We must be aware of when data is transferred to a foreign jurisdiction to manage our information risk appropriately. This will ensure we consistently meet our legal obligations throughout the supply chain. This will ensure we have adequate data transfer mechanisms in place which are not undermined by local legislation. All personal data must be processed in a location which is recognised as having an adequate level of data protection. Where the processing location is inadequate, a valid transfer tool (such as Standard Contractual Clauses) must be implemented.	X	X	X	X	X	X
23	Data Subject Rights	You have formal procedures in place to manage Data Subject Rights (DSR) requests. Where required in relation to your services, you will provide all reasonable assistance to British Land within 3 calendar days. If the system is supported or maintained by your appointed sub-contractor, they must adhere to these standards to ensure supply chain security	There is a statutory obligation to respond to Data Subject Rights Requests without undue delay and within 30 calendar days. For British Land, or the supplier in a data controller capacity, to comply with this requirement, we require immediate support.				X	X	X

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
24	Consent Management	Where applicable to your services to British Land: - You keep consent requests separate from any Terms and Conditions. - You maintain an easily accessible record of all consents obtained, meeting the minimum requirements as detailed by the ICO. - You provide a mechanism (e.g., check box, submit button) that is clearly presented and requires an 'affirmative action' by the user. - You provide a link to an appropriate Privacy Notice at the point you capture consent. If the system is supported or maintained by your appointed sub-contractor, they must adhere to these standards to ensure supply chain security					x	x	x
25	Transparency	Where applicable: You display data privacy transparency information to users (e.g., Privacy notices) as required. The Privacy Notices provided are clear, concise and provide the relevant information in line with the guidance from the ICO. If the system is supported or maintained by your appointed sub-contractor, they must adhere to these standards to ensure supply chain security.	Privacy notices are a key requirement of the Transparency principle of UK Data Protection Act 2018 and UK GDPR.					x	x
26	Privacy Enhancing Techniques	Where applicable (normally while processing Personal Financial, Sensitive or Biometric data) You create logical separation of the data OR You apply pseudonymisation techniques OR You apply high levels of encryption to the Personal Data If the system is supported or maintained by your appointed sub-contractor, they must adhere to these standards to ensure supply chain security	The application of privacy enhancing techniques reduces the risk to data subjects in the event of an information breach. This is applicable to data held at all stages of the information lifecycle.				x	x	x

No.	Category	Standard	Guidance	Engagement Type					
				Physical Access (No Systems)	Access Premises to Operate BL Systems	Remote Access - BL Premises	Our Data - Third Party System	IaaS	SaaS
27	Data Retention	Your company has: procedures in place to allow for data to be regularly deleted / updated in accordance with a defined schedule. processes in place that allow for the irrevocable erasure or return of the data upon contract completion / termination. procedures in place to ensure that any personal data downloaded in the delivery of your services to British Land, via remote access or other means, is deleted after use. If the system is supported or maintained by your appointed sub-contractor, they must adhere to these standards to ensure supply chain security					X	X	X