IT Security Web Guide

Information Security Supplier Standard

Issue 1.0

Table of Contents

1 Overview

This document defines the standard which Jaguar Land Rover's supplier community must comply with when handling Jaguar Land Rover's information, or utilising information technology resources on behalf of Jaguar Land Rover.

The term JLR shall mean Jaguar Land Rover (JLR) and all of its affiliates. The term Supplier shall mean the service provider supplying IT goods or services, including the Supplier's employees and the Supplier's subcontractors. The use of the term third party means any party other than the Supplier and JLR.

This standard describes the minimum information security arrangements required for a Supplier to provide goods or services to JLR. Where security controls are specified, the Supplier must be able to demonstrate that the control is effective and auditable.

Should a Supplier require further clarification of any part of this standard they should engage directly with their JLR procurement representative.

2 Governance & Compliance

2.1 Governance

1	A Framework for Information Security must be documented and commitment demonstrated by the Supplier's governing body. The Framework should align to the corporate security policies and provide assurance that information risks are being adequately addressed.

2.2 Regulatory Compliance

1	A security compliance management process must be documented, which comprises information security controls derived from regulatory and legal drivers and contracts.
2	The Supplier may be required to collect information including Personally Identifiable Information (PII) data as part of its daily business operations. The handling and storing of PII data must comply with local and regional laws and legislation.

3 Human Resource Security

3.1 Employment Lifecycle

Information security requirements, as described below, must be embedded into each stage of the employment life cycle, specifying security related actions required during the induction of each individual, their ongoing management and termination of their employment.

1	Applicants for employment (including external individuals such as consultants, contractors, engineers and employees of external parties) must be screened (and vetted where legal) prior to commencing work (e.g., by taking up references, checking career history/qualifications and confirming identity, such as by inspecting a passport).
2	Information security responsibilities for all employees throughout the organisation must be specified in job descriptions, terms and conditions of employment (e.g., in a contract or employee handbook) and performance objectives.
3	There must be a requirement for employees to accept terms and conditions of employment in writing, and for external individuals (e.g., consultants, contractors, engineers and employees of external parties) to sign non-disclosure/ confidentiality agreements.
4	There must be a documented requirement for access privileges to be revoked immediately when an authorised user: • no longer requires access to information systems (e.g., when changing role or moving to a different part of the organisation) • leaves the organisation
5	Upon termination of employment, internal and external individuals must be required to return assets (or equivalent) that belong to the organisation, including: • important documentation (e.g., about business processes, technical procedures and key contact details) stored on portable storage media or in paper form • equipment (e.g., mobile devices, laptops, tablets, smartphones, portable storage devices and specialist equipment) • software (including media, documentation and licensing information) • authentication hardware (e.g., physical tokens, smartcards and biometric equipment).

3.2 Ownership & Responsibilities

Ownership of critical business environments, processes, and applications (including supporting systems/networks) must be assigned to individuals (e.g., business managers), acknowledged and documented.

1	Individuals involved in implementing and maintaining systems which are being used to deliver services or goods to JLR must be: • assigned clear responsibilities • able to administer and use them correctly and deal with normal processing requirements • competent to deal with error, exception and emergency conditions • aware of information security principles and associated good practice • sufficient in number to handle required normal and peak workloads at all times.
2	Individuals who maintain systems which are being used to deliver services or goods to JLR must be supported by approved methods of: • administering users (e.g., adding new business users, updating access privileges, and revoking user access privileges) • monitoring key security-related events (e.g., system crashes, unsuccessful login attempts of authorised users, and unsuccessful changes to access privileges) • validating processes/data • reviewing error/exception reports • identifying potential security weaknesses/breaches (e.g., as a result of analysing user behaviour or patterns of network traffic).
3	The risk of individuals disrupting the running of business applications, systems and networks which are being used to deliver services or goods to JLR, either in error or by malicious intent, must be reduced by: • segregating the duties of individuals responsible for running business applications, systems and networks from the duties of those responsible for designing, developing and testing them • minimising reliance on key individuals (e.g., by automating processes, ensuring supporting documentation is complete and accurate, arranging alternative cover, job rotation and deputies for key positions) • organising duties in such a way as to minimise the risk of theft, fraud, error and unauthorised changes to information (e.g., by supervising and recording activities, prohibiting lone working and the segregation of duties).
4	The activities of individuals running business applications, systems and networks which are being used to deliver services or goods to JLR must be monitored (e.g., by providing supervision, recording activities and maintaining audit trails).

3.3 Remote Working

1	There must be documented standards/procedures covering individuals who handle JLR information when working in remote environments, including public areas (e.g., hotels, trains, airports and Internet cafes) or who work from home.

4 Security Awareness

4.1 Security Awareness Programme

1	The Supplier must promote good security behaviour throughout the organisation and establish a positive security culture.

4.2 Security Education & Training

1	Individuals must be educated/trained in how to run systems and applications correctly and how to develop and apply information security controls
2	Education/training must be given to provide business users with the knowledge and skills they need to correctly use any of the following to deliver services or goods to JLR: • business applications (including enterprise software, commercial-off-the-shelf software (COTS) and end user developed applications (e.g., those developed using spreadsheets)) • computer equipment (including desktop computers, laptops, tablets and smartphones) • specialist equipment (e.g., scanning devices, barcode readers, data capture appliances and monitoring equipment) • portable storage media (e.g., CDs, DVDs, magnetic tapes, hard disks and portable storage devices) • networking technologies such as local area networks (LANs), wireless local area networks (WLANs), Voice over IP (VoIP), Internet and Bluetooth • telephony and conferencing equipment, including teleconference and videoconference facilities (e.g., speakers, cameras and display screens) and collaborative online tools • office equipment, including printers and photocopiers, facsimile machines and scanners and multifunction devices (MFDs) • access control mechanisms (e.g., passwords, tokens and biometrics).
3	Education/training must be given to provide business users with the knowledge and skills they need for correctly: • creating and protecting electronic files used to deliver services or goods to JLR • classifying and labelling information used to deliver services or goods to JLR • removing unnecessary metadata * from electronic documents used to deliver services or goods to JLR • deleting unwanted information once no longer required • separating business and personal information

* *See next page*

** Electronic documents, such as word processed files, spreadsheets and presentations, can often include sensitive or inappropriate information, left unintentionally in electronic documents (often referred to as 'hidden data' or 'metadata'). Sensitive information, such as project names, customers' names, medical details and credit card numbers, could be accidentally disclosed to unauthorised parties in electronic documents in the form of:*

- *document properties (that might contain confidential comments, individuals' names and classification levels)*
- *tracked changes (that might contain private comments or potentially controversial statements)*
- *hidden rows, columns, sheets and database fields (that might contain customer or employee information, or credit card details)*
- *embedded objects (that might contain financial charts, private pictures and populated spreadsheets)*
- *header and footer information (that might contain project names and classification levels)*
- *hyperlinks (that might reveal sensitive information)*
- *ink annotations in electronic documents created using tablet PCs*
- *hidden confidential text or figures (e.g., coloured white).*

File cleansing software can be used to help identify confidential information that may be hidden within electronic documents.

5 Information Management

5.1 Information Classification

1	When handling JLR's information, Supplier organisations must comply with JLR's data classification requirements (see Appendix A Data Information Categories) and information encryption requirements (see Appendix B Data Encryption Requirements).
2	Supplier organisations may be required to enter into a Data Processing Agreement with JLR depending on their level of involvement with the handling of JLR information.

5.2 Information Privacy

1	Responsibility for managing information privacy must be established and security controls applied for handling personally identifiable information (i.e., information that can be used to identify an individual person). See Appendix A Data Information Categories.
2	There must be a documented information privacy policy that covers the: • acceptable use of personally identifiable information (PII) • requirements for protecting different types of PII • rights of individuals about whom PII is held • legal and regulatory requirements for privacy.
3	PII information must be: • handled in accordance with relevant legislation e.g., the EU Directive on Data Protection • protected throughout its life cycle i.e., through creation, collection, processing, storage (including backup and archiving), transmission, and destruction.
4	Where the Supplier handles or processes personal data/PII on behalf of JLR then the Supplier shall also comply with those JLR policies, standards and requirements in relation to such processing as may be published by JLR from time to time.

5.3 Information Protection

1	Documents containing JLR information must be handled in a systematic and structured manner to accommodate information security standards.

6 Asset Management

6.1 Hardware Lifecycle Management

1	There must be documented standards/procedures for managing the life cycle of hardware used to deliver services or goods to JLR. These standards/procedures must apply to all hardware acquired throughout the organisation.

6.2 Industrial Control Systems

1	Information systems used to deliver a service or product to JLR that monitor or control physical activities must be identified, categorised and protected by security arrangements that are tailored to operate in those environments.
2	An appropriate governance structure must be established to ensure that Industrial Control Systems* (ICS) used to deliver a service or product to JLR, and the environments in which they operate, are protected in line with the level of risk to the organisation and its risk appetite.
3	Roles, responsibilities and ownership for managing the information risks to ICS environments used to deliver a service or product to JLR must be clearly defined and agreed.
4	Information security arrangements related to ICS environments used to deliver a service or product to JLR must be prioritised, based on a comprehensive understanding of the: • organisation's reliance on each ICS environment • potential business impact of disruption to each ICS environment (e.g., financial, operational, reputational, or health and safety impact).
5	There must be documented standards/procedures for the protection of the organisation's ICS used to deliver a service or product to JLR.
6	ICS environments used to deliver a service or product to JLR (including associated enterprise IT systems) must be subjected to a rigorous information risk assessment, which may be combined/aligned with an operational risk assessment. The information risk assessment must determine security requirements for the ICS environment.

** Industrial Control Systems (ICS) is an overarching term that covers many different types of systems that monitor and control physical activities and environments. These types of system are also being referred to as operational technology (OT). The most common types of ICS include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC).*

Organisations typically rely on ICS to support business operations, such as: manufacturing and assembling products; providing energy, water and public transport; delivering goods to customers; and maintaining and supporting service equipment.

6.3 Employee Owned Devices

1	It is not permitted to store JLR's information on employee-owned devices (including smartphones, tablets and laptops).

6.4 Mobile Devices

1	Mobile Device Configuration Mobile devices (including laptops, tablets and smartphones) used to access JLR information must be built using standard, technical configurations and subject to security management practices to protect information against unauthorised disclosure, loss and theft.
2	Mobile devices used to access JLR information must be configured to log important events (e.g., unusual application behaviour, system crashes, and unsuccessful login of authorised users, unsuccessful changes to access privileges and unauthorised copying of sensitive information to portable storage media).
3	Mobility Device Management Smartphones, tablets and other devices used to access JLR information using mobile operating systems (e.g.: IOS, Android, Windows Phone, Blackberry) and the applications (‚apps') that run on them, must be protected in the event of loss, theft or cyber-attack by deploying appropriate mobile device management controls, which must include the ability to : • remotely wipe corporate mobile devices • block jailbreaking* on any mobile device which will be used to access JLR's information. * *The capability to modify a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator, thus allowing the installation of unauthorised software.*
4	Mobile Device Connectivity Mobile devices (including laptops, tablets and smartphones) used to access JLR information must be provided with secure means of connecting to other devices and to networks.

6.5 Portable Storage Devices

1	The use of portable storage devices (e.g. USB memory sticks, external hard disk drives, media players and e-book readers) to store JLR's information must be subject to approval by your JLR representative.
2	Portable devices approved to store JLR information must be encrypted using an appropriate cryptographic solution. See 12.1.3

3	Users of portable storage devices utilised to store JLR's information must be prohibited from: • sharing the device with unauthorised individuals • disclosing passwords (for accessing the device and encrypting files) to unauthorised individuals.

7 Access Management

7.1 Identity and Access Management

1	Identity and access management arrangements must be established to provide effective and consistent user administration, identification, authentication and access control mechanisms for business applications, systems, networks and computing devices which are used to deliver services or goods to JLR.

7.2 Access Control

1	Before access privileges are granted, authorisations must be checked to confirm access privileges are appropriate.
2	Access control arrangements must be established to restrict access to business applications, systems, networks and computing devices which are used to deliver services or goods to JLR by all types of user, who must be assigned specific privileges to restrict them to particular information or systems. At all times the principle of least privilege must be applied.
3	Access privileges must not be assigned collectively (e.g., using identifiers such as User Ids or authenticators such as passwords that are shared in a group) unless special circumstances apply. Whenever they need to be assigned collectively, this must be documented, approved by an appropriate business representative and subject to additional controls (e.g., restricted access privileges and contractual conditions).
4	Additional controls must be applied to special access privileges.
5	A process for terminating the access privileges of users must be established and actioned in a timely manner.

7.3 Access Control Mechanisms

1	Access to business applications, systems, networks and computing devices which are used to deliver services or goods to JLR must be restricted to authorised individuals by the use of access control mechanisms and reviewed regularly.

7.4 Access Control Mechanisms Passwords

The controls for Sections 7.4, 7.5 and 7.6 should reflect the current Industry Standard. The following examples represent the minimum requirements based on use cases.

1	Target environments (e.g., business applications, systems or network devices which are used to deliver services or goods to JLR) that are configured with access control mechanisms based on passwords, must require users to provide a valid UserID and password before they can gain access to them.
2	Users of access control mechanisms based on passwords must be advised to: • keep passwords confidential (e.g., avoid making them visible to others by writing them down or disclosing them to others) • change passwords that may have been compromised • report if passwords have been, or are suspected of being, compromised

7.5 Access Control Mechanisms Tokens

1	Target environments (e.g. business applications, systems, network devices which are used to deliver services or goods to JLR) configured with access control mechanisms based on tokens, must require users to provide a valid token (physical, soft token or smart card) and any related authentication information before they are granted access to the environment.
2	There must be a robust, secure process for registering new token users and issuing them with a token.

7.6 Access Control Mechanisms Bio-Metric

1	Target environments (business applications, systems, network devices which are used to deliver services or goods to JLR) that are configured with access control mechanisms based on bio-metric , must require users to provide a bio-metric response (e.g. fingerprint /vein recognition, iris/retina patterns or voice recognition) before they can be granted access to them.
2	There must be a process to register user's bio-metrics.
3	There must be a secure method to allow users to authenticate in the event of a failure in bio-metric authentication.

7.7 Sign-On Process

1	Users must be subject to a robust sign-on process before being provided with access to business applications, systems, networks and computing devices which are used to deliver services or goods to JLR.

8 Network Management

8.1 Network Device Configuration

1	There must be documented standards and procedures for configuring network devices.
2	Network devices must be subject to standard security management practices.
3	Access to network devices must be restricted a limited number of authorised, technically competent personnel, using access controls which support individual accountability and be protected from unauthorised access.

8.2 Physical Network Management

1	Networks including, voice networks, must be protected by robust physical controls and be supported by accurate, up to date documentation and labelling of essential components.
2	Network documentation (e.g., diagrams, inventories and schedules) must clearly identify high-risk environments and data flows that could lead to significant business or legal compliance impact should they be compromised.

8.3 Wireless Access

1	There must be documented standards/procedures for controlling wireless access to the network.

8.4 External Network Connections

1	There must be documented standards/procedures for managing external network access to the organisation's information systems and networks.
2	Information systems and networks accessible by external connections must be designed to: • use an agreed set of security controls for information formats and communications protocols • protect sensitive information stored on information systems and transmitted to external party locations
3	Information systems and networks accessible by external connections must: • restrict external network traffic to only specified parts of information systems and networks • restrict connections to defined entry points (e.g., specific network gateways)

4	External access to information systems and networks (e.g., via Internet connections) must be restricted by: • establishing 'Demilitarised Zones' (DMZs) between untrusted networks, such as the Internet and internal networks • routing network traffic through firewalls e.g., stateful inspection firewalls (typically located in the perimeter of a network) or proxy firewalls (typically located between internal networks) • limiting the methods of connection • granting access only to specific business applications, information systems or specified parts of the network
5	External access to information systems and networks must be subject to strong authentication.

8.5 Firewalls

1	Network traffic must be routed through a properly configured firewall prior to being allowed access to networks, or before leaving networks.
2	Networks must be protected from malicious traffic on other networks or sub-networks (internal or external) by one or more firewalls.
3	There must be documented standards/procedures for managing firewalls (or similar devices capable of filtering network traffic, such as switches and routers).

8.6 Remote Maintenance

1	Remote Maintenance of critical systems and networks must be restricted to authorised individuals, confined to individual sessions and subject to regular review.

9 Electronic Communications

Electronic communications encompasses any computer based activity including (but not limited to): Email, Instant Messaging (IM), Voice Over IP (VOIP), telephony and conferencing, any Internet based activity and Social Media.

9.1 Electronic Mail

1	Email systems must be protected by a combination of policy, awareness, procedural and technical security controls.
2	Email messages must be scanned for attachments that could contain malicious content.
3	There must be documented standards/procedures for the provision and use of email.
4	Mail servers must be configured to prevent the accidental disclosure of email and attachments to unauthorised individuals.
5	Email messages must be scanned for attachments that could contain malicious code.
6	Email systems must protect messages by verifying the source of senders' emails.

9.2 Instant Messaging

1	There must be documented standards/procedures for instant messaging services.

9.3 Voice Over IP (VOIP)

1	VOIP networks must be approved and protected by a combination of general network and VOIP specific controls.
2	There must be documented standards/procedures for VoIP applications and underlying technical infrastructure.
3	General network security controls for VoIP must be applied restricting access to VoIP networks to authorised devices.

9.4 Telephony and Conferencing

1	Telephony and Conferencing facilities must be protected by a combination of physical and logical controls, and regularly monitored.

10 System Management

Computer system, network and telecommunications installations (e.g. data centres) must be designed to cope with current and predicted information processing requirements and be protected using a range of in-built security controls.

10.1 Computer and Network Installations

1	There must be documented standards/procedures for information system, network and telecommunication installation designs, which require: • designs to take account of security architecture principles, business and security requirements • compatibility to be maintained with other information systems, networks and telecommunication installations used by the organisation • information system, network and telecommunication installations to be designed to cope with foreseeable developments in the organisation's use of IT (e.g., growth projections or adoption of open/proprietary standards).
2	Networks must be designed to: • incorporate the use of security domains and virtual local area networks (VLANs) to segregate information systems with specific security requirements or different levels of trust (e.g., employee-owned devices and devices used by consultants, contractors and employees of external parties) • employ firewalls in a manner that prevents them from being bypassed • allow access only to 'trusted' devices by preventing unauthorised devices from connecting to networks.

10.2 Physical Server Configuration

1	Servers must be configured to function as required, and to prevent unauthorised or incorrect updates.
2	Servers must be configured in accordance with documented standards/procedures.
3	Servers must be protected against unauthorised access.

4	Servers must be subject to standard security management practices, which include: • restricting physical access to a limited number of authorised individuals (e.g., by locating them in protected data centres or dedicated, locked storage rooms) • keeping them up-to-date (e.g., by applying approved processes for change management, vulnerability management, and patch management) • maintaining up-to-date malware protection software (including program code and signature files) to prevent infection by malicious software (e.g., computer viruses, worms, Trojan horses, ransomware, spyware, rootkits, botnet software and keystroke loggers) • applying a comprehensive set of system management tools (e.g., maintenance utilities, remote support, enterprise management tools and backup software) • monitoring them (e.g., using Simple Network Management Protocol (SNMP)) so that events such as hardware failure and attacks against them can be detected and responded to quickly and effectively • using secured technologies such as SSH, S-FTP, SSL, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, and FTP • reviewing them on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed on the server (e.g., by inspecting application records and event logs).

10.3 Virtual Server Configuration

1	Virtual servers must be deployed, configured and maintained in accordance with documented standards/procedures.
2	Virtual servers must be protected by applying standard security management practices to hypervisors, which include: • applying a strict change management process (e.g., changes are validated, tested and deployed within a critical timeframe) to help ensure the hypervisor remains up-to-date • monitoring, reporting and reviewing administrator activities to help ensure actions and privileges that they are allowed to perform are specifically aligned to their duties • restricting access to the virtual server management console (or equivalent) to a limited number of authorised individuals (e.g., virtual server administrators) • monitoring network traffic between different virtual servers and between virtual servers and physical servers to detect malicious or unexpected behaviour and known attacks.
3	Each virtual server must be protected by applying standard security management practices including; restricting physical access, system hardening, applying change management and malware protection, monitoring and performing regular reviews, and applying network-based security controls (e.g., firewalls, intrusion detection and data loss prevention).

10.4 Network Storage

1	Network Storage systems must be protected using system and network controls.
2	Network storage systems, such as Storage Area Network (SAN) and Network-Attached Storage (NAS) must be deployed, configured and maintained in accordance with documented standards/procedures.
3	Network storage systems must be subject to standard security management practices (e.g., restricting physical access, performing system hardening, applying change management and malware protection, monitoring them and performing regular reviews).

10.5 Service Level Agreements (SLAs)

1	Computer and network services that support critical business processes and applications must only be obtained from service providers capable of providing required security controls and be supported by documented contracts, or service level agreements.

10.6 Performance and Capacity Management

1	Business applications, systems and networks must be monitored continuously and reviewed from a business users perspective.

10.7 Backups

1	Backups of essential information and software must be performed on a regular basis, according to a defined cycle, and regularly tested.

11 Operational Security

11.1 Malware Protection

1	Systems throughout the Supplier organisation must be safeguarded against all forms of malware by maintaining up to date malware protection software which is supported by effective procedures for managing malware related security incidents.

11.2 Information Security Incident Management

1	An information security incident management framework must be established, including relevant individuals, information and tools required by the organisation's information security incident.
2	Information security incidents must be identified, responded to, recovered from, and followed using an information security incident management process.
3	Information security incidents must be immediately communicated to the JLR Security team.

12 Cryptography

12.1 Cryptographic Solutions

1	All JLR information classified as Confidential or Secret, or containing PII or SPII, must be encrypted when in transit or at rest. See Appendix B Data Encryption Requirements
2	Appropriate cryptographic solutions must be used when handling sensitive (i.e., Confidential, Secret or containing PII or SPII) JLR information. See Appendix A Data Information Categories
3	The selection and implementation of a cryptographic solution must take into account the legal aspects of using encryption, and include: • identifying legal obligations (for relevant jurisdictions) • assessing the risks (including legal risks) associated with using cryptographic solutions (including encryption algorithms) • selecting a suitable cryptographic solution (e.g., that meets legal, regulatory and industry standards)

12.2 Cryptographic Key Management

1	Cryptographic keys used to protect JLR information must be managed securely, in accordance with documented standards/procedures, and protected against unauthorised access or destruction.
2	There must be documented standards/procedures for managing cryptographic keys used to protect JLR information.
3	A documented operational process for managing cryptographic keys used to protect JLR information must be established.
4	Cryptographic keys used to protect JLR information must be protected against: • access by unauthorised individuals or applications • accidental or malicious destruction • unauthorised copying

12.3 Public Key Infrastructure

1	Where a public key infrastructure (PKI) is used to protect JLR information, one or more Certification Authorities (CAs) and Registration Authorities (RAs) must be established and protected.
2	A PKI used to protect JLR information must be supported by documented standards/procedures.

3	A PKI used to protect JLR information must be supported by establishing a root CA to: • generate public key certificates (digital certificates) • revoke public key certificates • publish public key certificates and certificate revocation lists (CRLs) in directories (or equivalent) • archive public key certificates and certificate revocation lists in an archive database (or equivalent).
4	The private keys of important internal CAs (and related sub-CAs) used to protect JLR information must be adequately protected to avoid unauthorised access.

13 Security Monitoring

13.1 Vulnerability Assessment

1	A process must be established to identify and assess the vulnerabilities and relevant controls in any environment which is being used to deliver a service or product to JLR.

13.2 Risk Evaluation

1	Information risk related to the delivery of any product or service to JLR must be evaluated based on analysis of threats, vulnerabilities, controls and business impact.

14 Security Audit

14.1 Security Audit Planning

1	Security audits of target environments which are used to deliver services or products to JLR, must be subject to thorough planning, which includes identifying risks, determining audit objectives, defining the approach and scope of security audits, and preparing a security audit plan.

14.2 Security Audit Management

1	The information security status of target environments (e.g., critical business environments, processes, applications and supporting systems/networks) which are used to deliver services or products to JLR, must be subject to thorough, independent and regular security audits.

14.3 Security Audit Reporting

1	The results of security audits of target environments which are used to deliver services or products to JLR, including findings and recommendations, must be documented and reported to stakeholders.

14.4 Remediation

1	Actions to address security audit findings must be incorporated into a programme of work and monitored to evaluate and review progress against audit findings, track associated results and actions, and conduct follow-up reviews to validate any remediation activity.

15 Business Applications

15.1 System Development Methodology

1	Development activities associated with the delivery of goods or services to JLR must be conducted in accordance with a documented system development methodology.

15.2 System Development Environments

1	System development activities associated with the delivery of goods or services to JLR must be performed in specialised development environments, which are isolated from the live and testing environments, and protected against unauthorised access.

15.3 Quality Assurance

1	Quality assurance of key security activities must be performed during the system development lifecycle of systems which will provide goods or services to JLR.

15.4 System Design

1	Information security requirements must be considered when designing systems which will be used to deliver goods or services to JLR.

15.5 Software Acquisition

1	Software used to deliver goods or services to JLR must be robust and reliable, and only acquired following consideration of security requirements and identification of any security deficiencies.
2	Suppliers assisting in providing goods or services to JLR must provide assurance that they can meet security requirements (e.g. by producing results of penetration tests, secure code review and vulnerability assessments, demonstrating adherence to standards, and providing an effective method for delivering software patches/fixes).

15.6 System Build

1	System build activities, including program coding and software package customisation, in relation to the delivery of goods or services to JLR, must be: • carried out in accordance with industry good practice • performed by individuals who have adequate skills & tools • inspected to identify unauthorised modifications or changes.

15.7 System Testing

1	Systems under development, including application software packages, system software, hardware, communications and services, which will be used to deliver goods or services to JLR, must be tested in a dedicated testing area that simulates the live environment, before the system is promoted to the live environment.

15.8 Security Testing

1	Systems under development which will be used to deliver goods or services to JLR, must be subject to security testing using a range of attack types (including vulnerability assessments, penetration testing and access control testing).

15.9 System Promotion

1	Rigorous criteria must be met before new systems, which will be used to deliver goods or services to JLR, are promoted into the live environment.

15.10 Post Implementation Review

1	Post-Implementation reviews (including coverage of information security) must be conducted for all new systems which will be used to deliver goods or services to JLR.

15.11 System Decommission

1	Systems, which have been used to deliver goods or services to JLR, that are no longer required must be evaluated, and subject to a decommissioning process, where required, taking account of relevant information, software, services, equipment and devices.
2	The decommissioning process must include the secure deletion of any JLR information.

15.12 Use of Cloud Computing

1	The use of cloud computing to deliver goods or services to JLR must include risk assessment to define the security controls required to protect information (stored or accessed via the cloud environment) from being exposed to unauthorised access, or regulatory non-compliance.
2	Appropriate contracts must be in place with third parties to manage any additional risk posed by the use of cloud computing environments to deliver goods or services to JLR.
3	The use of cloud computing must be approved by an appropriate JLR representative.

16 Supply Chain Management

Information risks must be identified and managed throughout all stages of the relationship with external suppliers, including organisations in the supply chain.

1	There must be a documented process for managing the information risks associated with external suppliers, including organisations within the supply chain who will assist in delivering goods or services to JLR. The process must be incorporated into the organisation's procurement process and include: • identification of critical and sensitive information • determining any additional security requirements • evaluating the bidding suppliers' ability • appetite to meet the organisation's security requirements • establishing a method for exiting, terminating, renewing and renegotiating contracts with external suppliers and providing alternative arrangements in the event that an external supplier becomes unavailable.
2	Evaluation of suppliers who will assist in delivering goods or services to JLR must include the identification and classification of any JLR information that will be shared with and accessed by third party organisations.
3	Contracts with external suppliers who will assist in delivering goods or services to JLR, must include obligations and security arrangements which specify: • approval for any outsourcing or sharing of JLR's information • the requirements for downstream third party organisations in the supply chain to meet the same security requirements as the primary supplier • the need for performance and security monitoring • the expedient reporting of any security incident back to JLR via the supply chain.

17 Business Continuity

A business continuity strategy covering the whole Supplier's organisation must be established. This strategy:

- promotes the need for business continuity management
- embeds business continuity management into the organisation's culture

17.1 Business Continuity Plans

1	Business continuity plans must be developed and documented to support all critical business processes throughout the Supplier organisation which might impacts their ability to deliver goods or services to JLR.

Appendix A Data Information Categories

Information Category	Description	Examples
JLR Public Data	Information that is authorised for public dissemination by Jaguar Land Rover.	Data which is intended for public use as defined by approved Jaguar Land Rover business functions. *Your Jaguar Land Rover representative will be able to assist in clarifying if this type of data is being managed as part of this engagement, if required.*
JLR Proprietary Data	Information created or obtained in the normal course of business and not classified as Secret, Confidential or Public that if disclosed to the public may cause some negative consequence to Jaguar Land Rover's business.	*Your Jaguar Land Rover representative will be able to assist in clarifying if this type of data is being managed as part of this engagement, if required.*
JLR Confidential Data	Information that supports Jaguar Land Rover's technical or financial position and which, if disclosed without authorisation, could cause damage to the Company.	*Your Jaguar Land Rover representative will be able to assist in clarifying if this type of data is being managed as part of this engagement, if required.*
JLR Secret Data	Information of a strategic nature that, if disclosed without authorisation, would cause substantial, severe, or irreparable damage to the Jaguar Land Rover, or its relationships.	*Your Jaguar Land Rover representative will be able to assist in clarifying if this type of data is being managed as part of this engagement, if required.*
Personally Identifiable Information (PII)	PII is any information that alone or used in conjunction with other information can be used to identify a living individual and provide information related to them in a "biographical" sense. *Information relates to an individual in a "biographical sense" if: (1) the content tells you something about a person (e.g. their financial or professional situation) or allows you to learn, decide or record something about an individual; or (2) your use of the information could have an impact on an individual.*	PII includes a person's name or other identifier combined with, for example, contact details (e.g. address, phone number, email address, etc.), date of birth, statements of opinion or intention about the individual, driving behaviours associated to a VIN/license plate number, geo-location data*, bank account or debit/credit card details*, salary* or payroll information etc. ** As a matter of internal policy (or where required by local laws), JLR reserves the right to classify these as SPII.*

Information Category	Description	Examples
Sensitive Personally Identifiable Information (SPII)	SPII is a subcategory of PII which is particularly privacy sensitive or could cause substantial harm or distress if lost or misused.	SPII includes: the racial/ethnic origin, political opinions, religious or other personal beliefs, trade union memberships, physical/mental health condition, sexual orientation, information related to criminal offences, or criminal proceedings/sentencing, National Insurance, social security and other government issued identification numbers; health care credentials and passport or other national identification information (including driving license), geo-location data, bank account or debit/credit card details, salary or payroll information, photographs, genetic or biometric data* (Inc. retinal/iris scans, fingerprints) etc.
Intellectual Property	Intellectual Property (IP) is the term given collectively to patents, registered designs, trademarks and copyright.	Intellectual Property might include research material, product designs, trademarks, software, or any other patented, registered designs, trademarks or copyrighted material.
Industrial Control Data	Data pertaining to Industrial Control Systems	Industrial Control Systems: Supervisory Control And Data Acquisition (SCADA) systems; Distributed Control Systems (DCS); Programmable Logical Controllers (PLCs) - including Manufacturing and Engineering devices; Confidential Manufacturing processes; or Confidential Manufacturing Systems data.

Appendix B Data Encryption Requirements

See Appendix A for descriptions of the information categories.

Information Category	Encrypt at Rest	Encrypt in Transit
JLR Public	No	No
JLR Proprietary	No	No
JLR Confidential	Recommended	Recommended
JLR Secret	Yes	Yes
PII	Yes	Yes
SPII	Yes	Yes