JLT GROUP
SECURITY STATEMENT

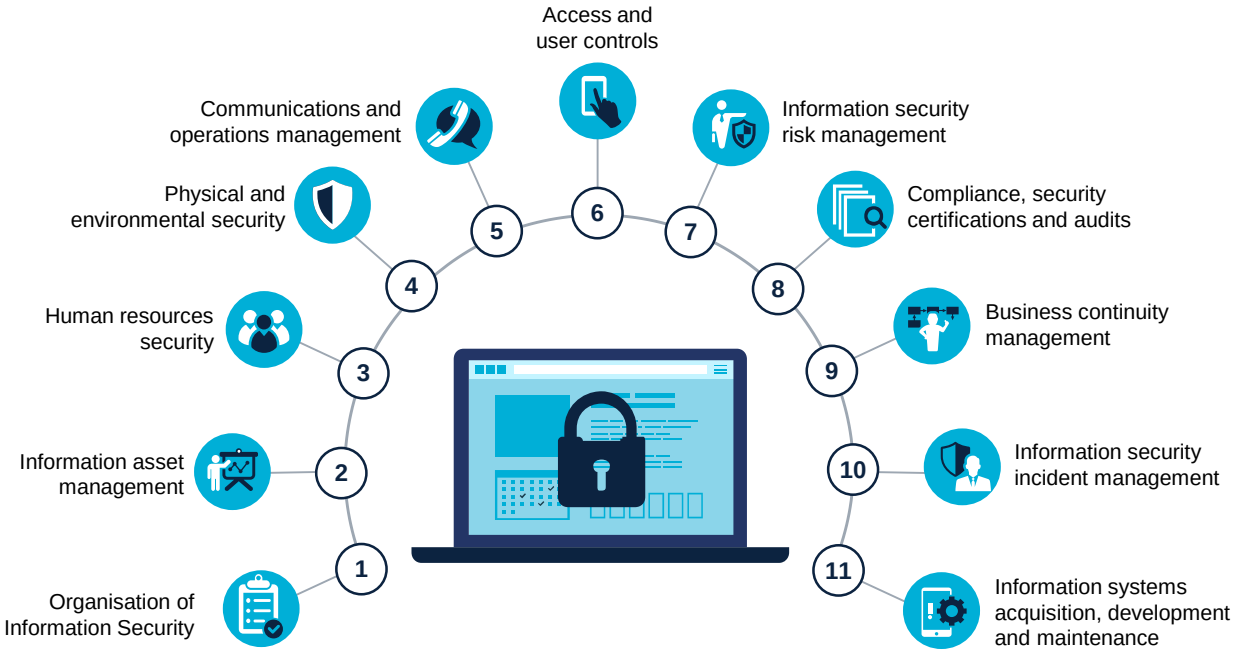
JLT SECURITY STATEMENT

We take data security seriously. To reflect this, we've put in place a clear chain of responsibility when it comes to security. Our JLT Group Chief Information Security Officer (CISO) and CISO office is responsible for helping all JLT entities protect data and technology assets, and manage security risks. The CISO office does this by developing, monitoring and reviewing our information security framework policies and standards.

How we protect our data and technology assets

To check that the management of security is effective, all information security policies are produced and governed as part of the group-wide policy framework. We deploy these across the group through our Chief Operating Officer (COO) and Chief Information Officer (CIO) office structure.

We review our group information security polices regularly and publish them through the JLT group policy portal. These policies underpin a standard information security management system framework that we've designed across the following areas. You can read about each of these areas in detail below.

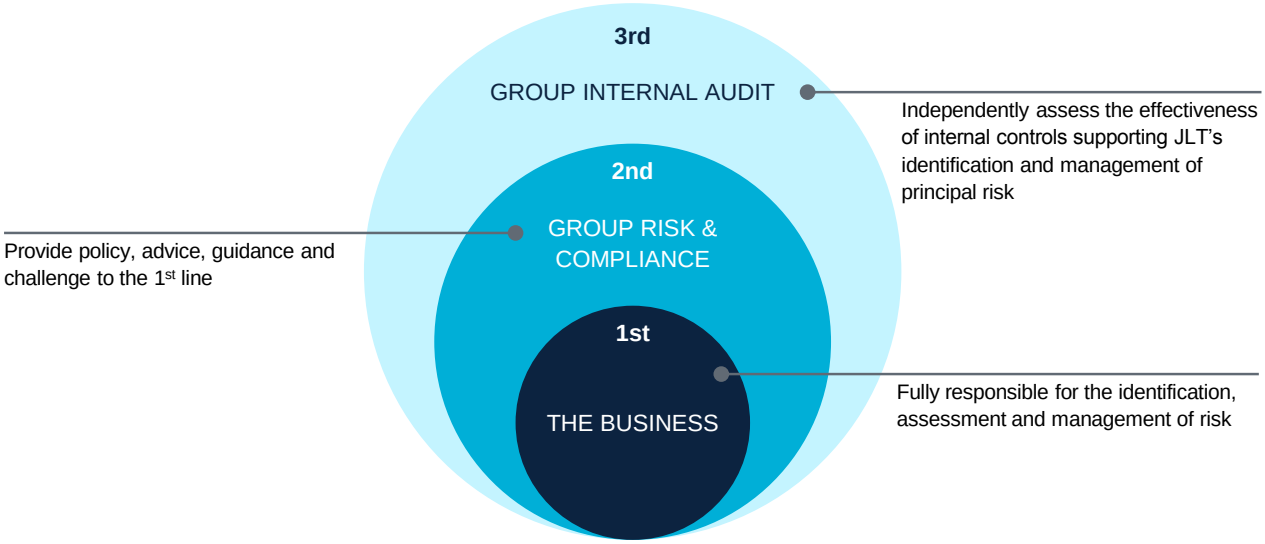


Our group information security policies are backed up by a formal set of standards. These standards set out the minimum requirements that our business units must meet when they implement controls to comply with this information security policy.

THE INFORMATION SECURITY FRAMEWORK AREAS

1 Organisation of Information Security

We have a JLT Group CISO who reports equally to the Group Chief Risk Officer (CRO) and the Group CIO. This is the second line of defence within our 'Three Lines of Defence' governance model.



Our Group CISO office oversees our business information security officers. These officers provide a more detailed level of support and are spread across all major geographic regions.

The Group CISO also works within the group governance model to make sure that the following teams understand our security risk position:

- The Group Executive;
- The Group and Business Board;
- The Group Operating Committee; and
- The Group Audit and Risk Committee.

2 Information Asset Management

As regulation has evolved, we've put a formal categorisation structure in place for our information assets across the group. We have four levels of classification and these apply at a user level and a company level. You can see this structure in the table, below. It supports the control design, security needs and handling of information assets throughout their lifecycle.

Classification	Public	Internal	Confidential	Highly Confidential
Examples	JLT Marketing Material	JLT Internal Policies and Procedures	All client data and all Personal Data that is not deemed highly confidential	Medical related information, trade union membership, mergers and acquisition information.

3 Human Resources Security

We know what an important part people play in terms of our cyber resilience and security capability. So we've broken our management of this issue into three areas:

Joiners and recruitment

We carry out standard checks and enhanced vetting, including CRB checks in the UK. We use financial sanction lists for anyone who might be a risk in relation to customer data or financial crime. We ask for educational certificates and verify any details of training from previous employers. And we'll ask people to fill in any details if there are gaps in their CV.

Training and information security awareness

During inductions, we tell our staff all about our information security policies and how important they are. And our employee handbook reinforces their roles and responsibilities. We run mandatory annual online refresher courses and use other tools, like phishing tests.

Role changes and leavers process

We have a formal joiners / movers / leavers policy and process in place and we use automation technologies where we can. This includes direct management oversight and accountability to ensure their employees only have access to data that they need for their role and that all security steps are followed when they leave.

4 Physical and Environmental Security

We've broken down our approach to physical and environmental security into three broad categories:

Data centre security

We follow the ANSI tier 3 industry standard, providing n+1 power, redundant cooling and 24/7 security with connectivity to a wealth of technology partners and providers. We use world class co-location facilities operated by well-known and respected global data centre providers. These facilities conform to all the normal industry standards and best practices for data centres. This includes full perimeter security, 24-hour security guards, electronic access controls, access logging and physical segregation between tenant areas within the machines rooms. Access to sensitive areas is logged electronically. If needed, our property services and security team can review these logs. And all server rooms and data centres have CCTV.

JLT office security

We secure entry and exit points at our locations. We give our employees access passes when they join, with their name and photo. Only authorised people can give others access to our offices. We keep a log of who accesses any sensitive areas. And our property services and security teams can review these logs if they need to.

Third party services security (including the cloud)

As part of our third party risk management framework we conduct information security due diligence on third parties. We look at the potential information security impacts associated with the service they're providing. In turn, this determines the level of detail and assurance we collect. We assign relationship managers to monitor our key suppliers and make sure we have on-going governance in place. And we set out all of our third party security requirements in our service delivery agreements.

5 Communications and Operations Management

We follow industry best practice design principles for our platforms and networks. And we use the Information Technology Infrastructure Library (ITIL) industry-standard framework for communications and operations management. This covers all phases of our service design, service transition and service operation. There's a comprehensive set of information security standards and procedures within that framework, including:

Protection of communications links

Private network access: We use Virtual Private Network (MPLS) technology with secure tunnels to provide office and data centre connectivity. We control LAN access at the port level and WIFI access by physical device ID.

Remote network access: We use 2-factor authentication to establish a secure connection to access services on the company LAN. Laptops can establish a secure link using the same system.

Protection of data in motion, at rest and data leakage controls

We look to encrypt data in motion and secure data at rest. We do this as a security design principle, assuming there are no technical limitations. We achieve this through a standard set of methods and technologies, which are dependent on the sending and receiving systems involved with transferring that data. All of the systems are based on industry standards and best practices. For data at rest (bearing in mind any technical limitations), we deploy encryption technologies at the hardware (including tapes and other removable media) and data storage layers.

We've put in place policies and standards to govern the transfer of data. This includes a broad data loss protection capability that uses both blocking and alerting methods. This capability is based on underlying technology capabilities, governed policies and rule sets.

We've made write access to removable media a controlled process.

General user controls

All of our employees, contractors and temporary staff are subject to a group-wide, all-employee, information security policy. This covers the acceptable use of technology resources, as well as rules for using approved technology solutions and services.

We've built our user devices to standard images, following good industry standards. And all of our laptops have full-disk encryption by default.

Hardening and patching controls

We manage all of our workstations and servers with a standard build. This includes installing software management agents which make sure any patches are deployed at the right time. The anti-virus (AV) patterns are updated automatically and we use a central management console to track and report on compliance of devices.

All of our servers, including application servers, have AV installed and are appropriately configured. We update patches and we have an emergency out-of-bounds change and release process to deploy any critical or urgent security updates and patches.

Security logging and monitoring controls

As well as monitoring data traffic coming into our estate by way of checkpoint firewall, we use a security information and event management (SIEM) solution with agents on all critical servers that constantly monitor for suspicious activity.

We receive reports of any attempted attacks on the network with full details of threats attempted to be exploited, along with IP listings.

Anti-malware controls

We have an industry-standard anti-malware/anti-virus system in place. We update it at least daily, or more often, if necessary.

We monitor, filter and govern how our people use the internet, using industry-standard solutions. And we've put in place an acceptable use policy.

Vulnerability scanning and penetration testing controls

We run scans to test for internal vulnerabilities. And we carry out penetration testing on our internet-facing applications at least once a year.

We subscribe to a number of vulnerability notification services including membership of the CiSP portal provided by the UK NCSC, as well as the official hardware and software manufacturers' feeds. We routinely apply patches, in line with the hardware and software manufacturers' recommendations. All of these patches are subject to our change management process for approval and testing, and when we apply the patch depends on how severe the defect is. We assess and grade each patch in terms of severity and implementation timescales.

6 Access and User Controls

We know how important clear and robust identity and access management is. In particular, we recognise the part it plays in the confidentially, integrity and availability of data. So, we've put in place policies for each of these areas:

Identity management

We manage our employees through our HR systems and processes to make sure we have unique identification in place. Because of this, we can interface with IT procedures, authentication processes and, where possible, identity and access management technology. This helps us to manage user accounts in a timely and appropriate way.

Authorised access and recertification

If someone wants access to our systems and applications, they need to make a request for a line manager to authorise. We give this access on a 'least privilege' and 'need-to-know' basis. And we recertify access to any systems that contain sensitive information. How often we review this access depends on how sensitive the information is.

7 Information Systems Acquisition, Development and Maintenance

We have put in place structured processes to look after the acquisition, development and maintenance of information systems.

For systems acquisition governance, our control and approval sits across the three primary layers of CIO, Chief Operating Officer and Chief Financial Officer. These people are also involved during the development and maintenance phases.

Where we develop the software ourselves, we follow a structured software development lifecycle (SDLC), which we've split into two broad sections. And we've included quality control checkpoints to govern the process.

Structured software development lifecycle

Pipeline and demand management

SCOPING:
We follow a robust up-front scoping and planning phase with agile development techniques to create a delivery roadmap. We also make sure that our system analysts and architects work closely with the product owner.

Release planning and delivery

REFINEMENT:
Once we've understood the requirements and estimates in detail, we put together a release plan.

DEVELOPMENT:
We turn the release plan into a release candidate. We use detailed design and development to create the solution and then confirm that it's ready for testing.

TESTING AND VALIDATION:
We use independent regression, performance and functionality testing to make sure that the release is ready for the customer.

LAUNCH:
We offer support once we've released the solution.

We maintain separate environments for test data. This stops anyone getting unauthorised access to information assets, or making changes to those assets.

In terms of maintenance and decommissioning, we follow standard practices that embed and integrate with our ITIL-aligned service model. These connect with the communications and operations management area of the framework.

Specifically, for the decommissioning phase, we've put the following controls in place:

- We dispose of any equipment securely, basing our process on the Waste Electrical & Electronic Equipment Regulations 2013. In terms of equipment destruction, we wipe any tapes then overwrite them, using our tape backup software. When we destroy any media, including tape and drives, we use a rigorous destruction process. This process is based on (IL6) of the HMG Infosec 5 Standard Manual 'S'.
- We record any hard drives, then store them securely, following a data de-classification process. We process the procedure using UK Government-approved equipment and secure HDD & DLT granulation to 3mm. This process destroys the hard disk drive and makes it impossible to retrieve any data.

8 Information Security Incident Management

Information security incident management is an embedded part of our ITIL-aligned service model.

It makes use of the procedures, capacity and tools that we have to deliver that model. We have dedicated security operations resources and specific security incident and event management tools.

STEPS WE TAKE IN A SECURITY EVENT

In parallel to the main process, for major security incidents, we put in place connections with our wider data breach and business continuity policies. This includes communication, analysis and documentation of the incident.

9 Business Continuity Management

Our approach to business continuity management and disaster recovery is supported by a group-wide approach to risk management, including business impact analysis. When it comes to security, we focus on two primary controlling factors:

- We locate our disaster recovery systems and services in a geographically diverse, on-premises data centre with redundant power, cooling and security facilities. This gives us high availability and protection 24/7.
- Our technology major incident management process is part of the group's business continuity framework. We've embedded information security (including cyber security) into our crisis management, business continuity and disaster recovery planning.

10 Compliance, Security Certifications and Audits

As a company regulated by the Financial Conduct Authority (FCA) audit, compliance and governance are at the heart of our operations. We're subject to regular independent financial and IT system audits by both internal and independent third party auditors.

We are Cyber Essentials certified and we align our Information Security Framework (ISMS) with ISO 27001. We also carry focused ISO 27001 certification within targeted business areas.

We make sure that all key IT service providers are secure and compliant. As part of our vendor management and third party risk management framework, we assure security alignment though auditing, inspection and the review of certificates and reports (such as SSAE 16 SOC 1 or SOC 2 type ii).

11 Information Security Risk Management (including cyber threat management)

For us, cyber risk is a board level issue. We regularly focus on information security risk through our group governance committees.

We take a technology and behavioural approach to cyber security, because of the nature, scale and complexity of the threats it poses. Because of this, our approach includes adopting industry good practice for IT security controls, process and policy, supported by training and awareness. Our cyber framework is based on ISO 27001 and the NIST cyber security standards, which are endorsed by the UK and US governments.

We also recognise that insurance is an important part of managing cyber risk. We have specific cyber insurance cover and we also augment that with retained partner arrangements for cyber legal and cyber forensics expertise and support.

Jardine Lloyd Thompson Group plc
The St Botolph Building
138 Houndsditch
London EC3A 7AW
Tel: +44 (0)20 7528 4444

www.jlt.com