Global Information Security Policy

ISP100

1 June 2018

Contents

Global Information Security Policy

Policy scope

The Global Information Security Policy addresses SDL's global security requirements and controls for IT Security, Information Security, Personnel Security and Physical Security. Detailed security requirements may be found in subordinate policies, processes and standards which comprise SDL's information security management system (ISMS).

This policy applies to all SDL permanent and temporary employees, including contractors, freelancers and those employed by SDL's suppliers as set out in their relevant contracts, in all locations and operations. It is the responsibility of each individual to remain conversant with, and implement the requirements of, this and any supporting policies.

Policy rationale

The Global Information Security Policy presents relevant and defining information about the objectives and functions of the SDL Information Security Program and how all of SDL's security elements contribute to SDL's global security posture. This document provides a high level view of SDL's control environment which is implemented to minimize malicious or unintended risks to the confidentiality, integrity and availability of SDL's assets, including people, facilities, equipment and information in all its forms. It is equally applicable to customer assets under the control of SDL. This document provides guidance to everyone with logical or physical access to SDL or customer information and facilities to assist them implementing good practice whilst carrying out their responsibilities.

Terms and definitions

Information Security Management System	All of the policies, procedures, plans, processes, practices, roles, responsibilities, resources, and structures that are used to protect and preserve information. It includes all of the elements that organizations use to manage and control their information security risks.
Information security policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Personally identifiable information (PII)	Any information about an individual maintained by an organization, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Sensitive PII	Information which, when disclosed, could result in harm to the individual whose privacy has been breached. Such information includes biometric information, medical information, personally identifiable financial information and unique identifiers such as passport or Social Security numbers.

Information security event	Identified occurrence of a system, service or network state indicating a possible breach of information security; policy or failure of controls; or a previously unknown situation that may be security relevant.
Information security incident	A single – or series – of unwanted or unexpected information security events that have significant probability of compromising business operations and threatening information security.
Fraud	A deliberate deception to secure unfair or unlawful gain.
Data breach	An information security incident in which sensitive, protected or confidential data has (potentially) been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve, personally identifiable information (PII), trade secrets or intellectual property.
Cloud Customer	An individual or entity that utilizes or subscribes to cloud-based services or resources.
Cloud Provider	A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations and/or individuals, usually for a fee, otherwise known to clients “as a service.”

Organization of Information Security

The Chief Transformation Officer (CTO) is the executive sponsor for (information) security and SDL’s Information Security Program. The CTO is chairman of the ISMS steering committee, which controls the definition and execution of the tasks to maintain the Information Security Program in a way that supports SDL’s business goals.

Day-to-day management of SDL’s Information Security Program is performed by the SDL Information Security, Privacy and Compliance (ISPC) Team. The SDL ISPC Team maintains the ISMS policies, performs security validation tests, manages security incidents, etc. The SDL ISPC Team consists of the Global Information Security Officer, the Information Security Officer, the Global Data Privacy Officer, the Lead Information Security Auditor, the Global IT Security Engineer and an Information Security Engineer.

Roles and Responsibilities

Security roles and responsibilities within SDL are identified below:

Chief Transformation Officer (CTO)

The CTO is the executive sponsor for the SDL Cyber Security and Privacy Program. The CTO is the ISMS Steering Committee chairperson and is responsible for the implementation of information security and privacy within SDL. The CTO discusses security and privacy concerns with the ISMS Steering Committee and the Global Information Security Officer, and informs SDL’s Executive Team about information security and privacy activities. The CTO represents SDL’s security and privacy concerns during capital planning and investment control processes by defining a discrete line item for information security and privacy in the budget.

Global Information Security Lead / Officer

The Global Information Security Officer is responsible for defining the security strategy for the entire SDL organization, as presented in SDL’s ISMS. The Global Information Security Lead is a member of the

ISMS Steering Committee and initiates regular steering committee meetings. The Global Information Security Lead provides oversight of the information security tasks required to maintain confidentiality, integrity and availability of SDL's systems and operations. The Global Information Security Lead must hold a Certified Information System Security Professional (CISSP) (or equivalent) certification and should attend relevant trainings and conferences to keep knowledge up to date.

Information Security Officer

The Information Security Officer –supports the Global Information Security Lead in the definition and implementation of the ISMS policies and procedures and the security activities of the SDL Information Security Program. The Information Security Officer should attend relevant trainings and conferences to keep knowledge up to date.

ISPC Information Security Engineer

The ISPC Information Security Engineer is responsible for implementation of the information security policies and procedures for the entire SDL organization. The ISPC Information Security Engineer also supports SDL employees with integration of information security into their day-to-day activities. The ISPC Information Security Engineer must hold or be working towards a Certified Ethical Hacker (CEH) certification and should attend relevant trainings and conferences to keep knowledge up to date.

Global Data Privacy Officer

The Global Data Privacy Officer is responsible for defining SDL's stance in privacy law adoption and the privacy law framework for SDL. The Global Data Privacy Officer is also responsible for maintenance of privacy related policy information in the ISMS. The Global Data Privacy Officer must hold or be working towards a Certified Information Privacy Professional – European Union (CIPP-EU) and Certified Information Privacy Professional – United States (CIPP-US) certification and should attend training and conferences to keep knowledge up to date.

Lead Information Security Auditor

The Lead Information Security Auditor is responsible for validation of the implementation and effectiveness of SDL's information security policies and procedures through auditing of SDL's systems, operations and supply chain. The Lead Information Security Auditor must hold or be working towards an International Register of Certificated Auditors (IRCA) certification and should attend training and conferences to keep knowledge up to date.

Global IT Information Security Engineer

The Global Information Technology (IT) Information Security Engineer works directly with Enterprise IT and is responsible for implementation of the information security and privacy policies and procedures for the SDL IT infrastructure. The Global IT Information Security Engineer also supports SDL employees with the integration of information security and privacy into their day-to-day activities. The Global Information Security Engineer must hold or be working towards a Certified Ethical Hacker (CEH) certification and should attend relevant trainings and conferences to keep knowledge up to date.

ISMS Steering committee member

All members of the ISMS steering committee actively participate in steering committees organized. Changes in current or new security policies are reviewed by the steering committee members.

All SDL Employees

All SDL employees are individually accountable and responsible for information security by maintaining an awareness of and following SDL's information security policies and profiles, reporting all potential and real security incidents when discovered and attending annual an updated information security training events.

Applicable Laws, Regulations, and Standards adopted by SDL

SDL uses the following laws, regulations, and standards for defining security in the ISMS:

- ISO 27001
- ISO 27002
- ISO 27017
- ISO 27018
- NIST CSF
- NIST SP 800-171
- NIST SP 800-53
- CSA CCM

SDL's Head of Group Legal will maintain the statement of Legal and Statutory requirements, which summarizes information security relevant regulatory requirements.

Information Security Management System

The SDL Information Security Management System (ISMS) comprises the people, processes and technologies employed at SDL regardless of whether they fall within an area of the organization which is in scope of the ISO27001 certification. Global Policies are used to define the high level requirements of the ISMS, outlining the effects to be achieved to support SDL's business aims. Supporting policies and standards are used to specify how the requirements of the ISMS will be met at the operational level.

Monitoring the ISMS

The ISMS is controlled by the Information Security Steering Committee (ISSC). Membership of the ISSC consists of a number of permanent members, which may change based on organizational requirements. Additionally, membership may be extended on an ad hoc basis to specialists where specific issues are to be discussed. Core membership of the ISSC includes:

- Chief Transformation Officer (Chair)
- Chief Product Officer
- Chief Financial Officer
- Executive VP Global Client Services
- VP Quality, Systems & Processes
- Global Information Security Lead / Officer
- Information Security Officer (Secretary)

The ISSC shall meet bi-monthly, though extraordinary meetings may be called as required. The ISSC shall identify the controls most critical to supporting SDL's business aims and decide the appropriate performance indicators for each, along with the team responsible for implementing, monitoring and reporting on control effectiveness. Effectiveness reports shall be produced at each meeting where the ISSC will consider the evolving threat environment and SDL's business aims to ensure control performance is adequately supporting the organization and that risks are appropriately addressed.

Security Risk Management

SDL's information security strategy supports SDL's aims by identifying, prioritizing and managing its security risks. Operational teams throughout the organization are responsible for identifying, assessing and managing their risks in accordance with SDL's Risk Management Policy (ISP101). Security and privacy risks are addressed through the application of appropriate security controls and associated risk treatment plans and the acceptance and management of residual risks. Oversight and governance of the risk management processes is exercised by the ISPC and ISSC as appropriate.

Further risk management guidance may be found in ISP101 – Risk Management Policy.

Governance

SDL operates in an environment where it must: comply with national and international laws, consistently demonstrating an effective ISMS to its external auditors; and be able to show, customers that its contractual security obligations are being met. Additionally, as threats constantly change and develop, so must SDL's controls whilst at the same time continuing to support business aims.

Therefore, SDL's ISMS must be kept under regular review to ensure that the policies and controls in place continue to support business aims by adapting to the changing threat landscape, incorporating any statutory or regulatory requirements is considered when applying and managing controls; that consequential risks are identified and appropriately managed; and that any changes to the legal or regulatory environment are incorporated. For these reasons SDL monitors the effectiveness of its controls by: conducting tests against its infrastructure, for example penetration or vulnerability testing; by collecting information on policy compliance, such as endpoint encryption and AV status; by conducting audits across the ISMS by its internal teams; and by exercising its contingency and response plans.

The results of these governance activities will be contained in reports distributed to the appropriate teams and their management and it is the responsibility of the control owners to ensure that any weaknesses are mitigated and managed.

Further audit and compliance information may be found in ISP102 – Security Testing Policy.

Logical Access

Access to SDL's systems and information must be controlled to protect its confidentiality, integrity and availability. Accordingly, access is restricted to those with a 'need to know' and is reviewed periodically to ensure appropriate access is maintained. Access credentials must meet specific minimum requirements, depending on the subject system, to reduce the risk of unauthorized access.

Further guidance can be found in ISP103 – Global Logical Access Control Policy.

Business Continuity

SDL has global presence and offers several SaaS products to its customers. The implementation of an effective Business Continuity policy ensures preparations are made to identify risks which may affect SDL's ability to operate during an incident and recover quickly in the aftermath. All SDL employees must ensure they understand the business continuity process and their place in it. Business continuity plans and processes must be regularly reviewed and tested to ensure effectiveness.

ISP104 - Business Continuity Policy covers SDL's strategy for business continuity and defines the scope, roles and responsibilities for Business Continuity across SDL.

Information Classification, Handling and Retention

Information assets created, stored and used within SDL have value, which must be identified by the asset owner or creator to allow the appropriate security controls to be applied. Additionally, information processed for customers in SDL SaaS products must be classified according to its value to the customer.

All employees are required to protect information according to the data classification assigned to it. Access to all classified information is based on the Need-to-Know principle. Although people might be authorized to access information, they should only access data when strictly required.

Further information classification, handling and retention information may be found in ISP105 – Global Classification and Handling Policy.

Security Incident Management

A risk-based approach to security focused on supporting business aims, such as that implemented by SDL, results in the likelihood that a security incident will occur at some point. Therefore all SDL employees must ensure they know how to identify and report a security incident and must be fully familiar with their involvement in the incident management process. SDL's security incident management processes must be in place and tested.

SDL's security incident management process follows a four stage approach focused on: Preparation; Detection & Analysis; Containment; Eradication & Recovery; and Post-Incident Activity. This supports SDL's business continuity policies and processes.

Physical Security

Information and assets at SDL facilities must be classified according to their organizational value and appropriately protected. SDL's physical security policy defines guidelines for the identification, assessment and management of physical security risks and the implementation of several security zones within the facility.

SDL's ISP107 – Global Physical Access Policy should be consulted for further information on physical security.

Data Privacy

SDL's employees handle a variety of Personal information for both other SDL employees and for customers. In some cases this personal information may fall into the category of sensitive information such as healthcare data, which requires increased levels of protection. In all circumstances, personal information and sensitive personal information must be processed and stored in accordance with SDL's policies and any local legislation.

SDL's Data Privacy Officer maintains a Privacy Legislation Framework to meet regulatory requirements for data privacy. The Privacy Legislation Framework covers relevant privacy legislation for SDL as a data controller and / or data processor.

Further data privacy information may be found in ISP108 – Privacy Policy.

Privacy Impact Assessment

The implementation of SDL's Privacy Legislation Framework, supports privacy by design. Part of privacy by design is the execution of a Privacy Impact Assessment to ensure proper protection of personal data.

ICT Systems Management

ICT Systems includes all ICT systems used by SDL in SDL's ICT infrastructure or SaaS products. SDL's requirements for ICT system installation and maintenance can be found in ISP109 – ICT Systems Management.

Customer owned ICT Systems

Customer owned ICT Systems (for example an on premise installation of an SDL product) are managed and maintained by the customer, this responsibility includes information security.
In case SDL employees are required to access such systems, customer's security requirements apply.

Cryptography

SDL uses cryptography to protect physical and logical assets. Cryptographic solutions must be employed correctly for them to be effective and cryptographic keys must be managed to ensure their availability. SDL's requirements for cryptography are contained in a number of Global policies, such as the Classification and Handling Policy (ISP105) and the Secure Software Development Policy (ISP112)

Further cryptography information may be found in ISP110 – Cryptographic Policy.

Vendor Management

SDL's supply chain constitutes a risk due to the reliance on a third party implementing appropriate controls to protect services and information. SDL's vendor on-boarding process must include an

information security assessment which varies in detail depending on the goods or services to be provided, or the level of physical or logical access provided to the vendor. Additionally, appropriate 'Right to audit' clauses must be contained in all vendor contracts which allow SDL to carry out periodic assessments of the effectiveness of a vendor's controls. Vendor contracts must also include a set of minimum expected security requirements for protecting SDL assets and information and an obligation for the vendor to inform SDL if they suffer a successful cyber-attack.

Further details can be found in the ISP111 – Global Vendor Security Assessment Policy.

Secure Software Development

Application source code and algorithms developed by SDL are considered Intellectual property. Such information is accessible on a Need-to-Know basis and requires specific security controls. Such controls are documented by teams holding such information.

Further secure software development information may be found in ISP112 – Secure Software Development Policy.

Training & Awareness

Information security training is provided to all SDL employees, contractors and vendors, through a variety of media. The ISPC is responsible for the content of the 'in house' training delivered within SDL and approves any externally provided training for specific roles. Completion of mandatory security training modules is monitored and reported to the ISSC for follow-up action as necessary.

- New hires are enrolled in the Atlas Learning Zone and are required to undertake the information security training within their first month of employment.
- Line managers are responsible for ensuring their teams are aware of and comply with any applicable security requirements.
- Annual training is provided through a number of short modules which are part of the mandatory Code of Conduct training.
- Think Security bulletins are distributed to all employees on a bi monthly basis or more frequently if necessary.
- Some specialists, such as software developers, are required to undertake specific training delivered through the MyLX portal.
- Other information security training courses are available to all employees.

Document Location

The source for this document can be found in SDL's ISMS and is accessible via https://sdl365.sharepoint.com/wa/ISP/ISMS/Shared%20Documents/ISP100%20General%20Information%20Security-Final.docx?d=w6995f777fe784553b69d400b87c96b2e

Document Control

Formal document version control and validation is managed via SharePoint.
However, document updates should be entered in this table by the person who makes the change.

Date	Author	Changes
27 January 16	J. Aijtink	Several changes were introduced: -New policy template -Made policy applicable for use in SDL
18 March 16	J. Aijtink	Processed review comments from ISPC team.
1 August 16	T. Shepherd	Reviewed and updated to reflect organizational changes.
10 January 17	ISPC Team	Annual document review completed.
20 September 17	R. Frith	Minor updates regarding definition of Global Information Security Lead. Removal of NA/SA Security Officer role and description.
1 June 18	E. Parkins	Reviewed and HITRUST controls incorporated as appropriate.

About SDL

SDL (LSE:SDL) is the global innovator in language translation technology, services and content management. With more than 25 years of experience, SDL delivers transformative business results by enabling powerfully nuanced digital experiences with customers around the world. Find out more at SDL.com.