Information Security Statement

Version number	3.7
Last Approved	Mar 12, 2024
Classification	PUBLIC

Overview

The Information Security Statement provides a framework that will ensure the protection of The Company's assets and its customers' data and privacy. The statement outlines the Information Security Mission and Strategy, as well as the security roles and responsibilities.

Applicability

The applicability of this statement falls under purview of the Security Documentation Overview.

Purpose

The Company recognizes that in order to deliver high-quality products and experiences to our customers as well as creating a first-class environment for its employees, it is necessary to examine and understand key criteria, such as:

- The vision and mission for The Company
- The Company's current place in the market
- Strengths and weaknesses, threats and opportunities
- The way that The Company operates as part of Learning Technologies Group

The Company's ***Information Security Mission*** is:

- to protect the confidentiality, integrity, and availability of the information assets of the company, its partners, and its customers through practices and infrastructure in a way that is aligned with The Company's business goals, risk posture, and ethics
- to enable business opportunity by aligning The Company's risk posture and security, privacy and compliance capabilities with the values and requirements of The Company's customers and prospective customers.

To fulfill this mission, The Company's ***Information Security Strategy*** is:

- to make Security and Privacy relevant, important, and easy for everyone at The Company by helping them to recognize, value, and successfully fulfill the security responsibilities of their individual roles
- to take a thoughtful, balanced, and adaptable approach to Security, informed by a continuous organization-wide dialogue and reassessment of security prioritiesScope

This policy applies to any electronic information storage and physical media containing sensitive or confidential data stored within The Company's hosted facilities or trusted subcontractors maintaining offsite or immutable online copies of systems and customer data. This

applies to all media including, but not limited to: disk drives, CDs, DVDs, magnetic tape, removable drives, memory cards and sticks, USB drives, and any other devices with persistent storage, both online or offline.

ISO 27001:2013 Control 4.1

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcomes of the ISMS.

ISO 27701:2019 Control 5.2.1

*The organization shall determine its role as a PII controller (including as a joint PII controller) and/or a **PII processor**.*

The organization shall determine external and internal factors that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS. For example, these can include:
— applicable privacy legislation;
— applicable regulations;
— applicable judicial decisions;
— applicable organizational context, governance, policies and procedures;
— applicable administrative decisions;
— applicable contractual requirements.

Where the organization acts in both roles (e.g. a PII controller and a PII processor), separate roles shall be determined, each of which is the subject of a separate set of controls.
NOTE The role of the organization can be different for each instance of the processing of PII, since it depends on who determines the purposes and means of the processing.

Scope

Defining governance processes for overseeing the following aspects of the information security and privacy program:

- Roles and responsibilities for security focused personnel, key stakeholders, and interested parties;
- Legal, regulatory and contractual obligations (including but not limited to);
  a. The EU General Data Protection Regulation (EU GDPR) 2016/679
  b. UK General Data Protection Regulation (UK GDPR) 2021
  c. EU-U.S. Privacy Shield Principles
  d. Swiss-U.S. Privacy Shield Principles
  e. The Foreign Corrupt Practices Act (FCPA)
  f. UK Bribery Act
  g. Family Educational Rights and Privacy Act
  h. California Consumer Privacy Act (CCPA - 2020)
- Hosting Operations and Security for all applicable SaaS offering systems and product lines, including both on premise and cloud hosted environments;
- Documentation, communication, performance and continuous improvement of these governance processes.

ISO 27001:2013 Control 4.3

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

ISO 27701:2019 Control 5.2.3

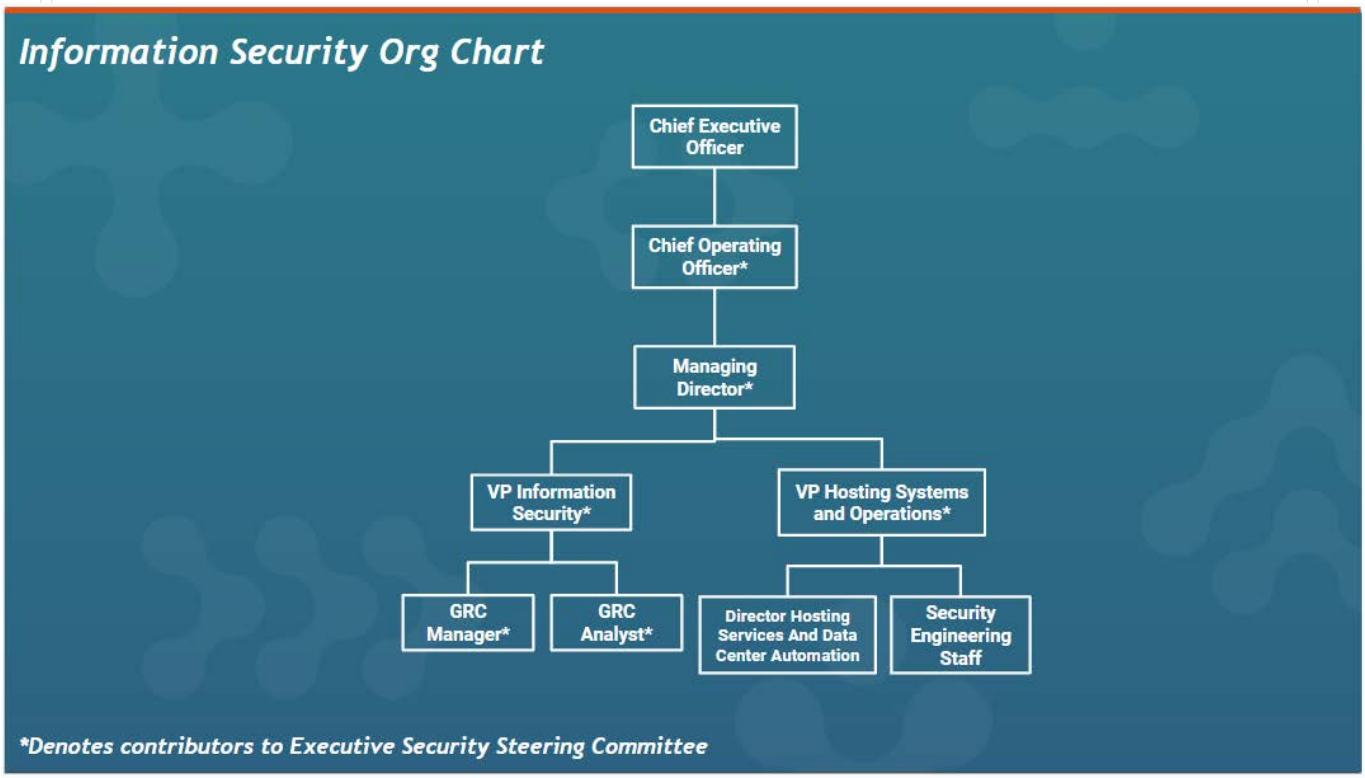
When determining the scope of the PIMS, the organization shall include the processing of PII.
NOTE The determination of the scope of the PIMS can require revising the scope of the information security management system, because of the extended interpretation of “information security” according to 5.1.

Roles, Responsibilities, and Obligations

It is the responsibility of all Personnel to comply with all applicable company policies and to appropriately utilize their assigned or accessed IT Resources to perform their duties and to meet The Company's business needs.

The below Org Chart denotes the separation of duties between the VP of Information Security, who is responsible for monitoring and enforcing security mechanisms, and the Security Team (within the Hosting department), who actively work to protect infrastructure and systems from threats.

Security Org Structure



The following outlines additional **role-specific** responsibilities:

- The **Managing Director** (with the involvement of Vice President of Customer Support and Services, Vice President of Professional Services, Vice President of Hosting Systems and Operations, Director of Human Resources – US, and Deputy General Counsel, and Director of Central IT Operations - LTG) is responsible for The Company's security and data privacy program, which ensures:
  - Information will be protected against any unauthorized access;
  - Confidentiality of information will be assured;
  - Integrity of information will be maintained;
  - Availability of information for business processes will be maintained;
  - Legislative and regulatory requirements will be met;
  - Business continuity plans will be developed, maintained, and tested;
  - Information Security training will be available for all employees;
  - All actual or suspected Information Security breaches will be reported to the **VP Information Security** and will be thoroughly investigated.
- The **VP Information Security** is responsible for developing acceptable use policies, audit and monitoring policies, and awareness training materials, as well as enforcing compliance with applicable policies and promoting continual improvement. The **VP Information Security** is responsible for safeguarding client and company data. Other responsibilities include:
  - Lead operational risk management activities to enhance the value of The Company and brand.
  - Oversee security personnel and vendors who safeguard The Company's assets, intellectual property and computer systems, as well as the physical safety of employees and visitors.
  - Identify protection goals, objectives and metrics consistent with the corporate strategic plan.
  - Manage the development and implementation of the information security policy, standards, guidelines and procedures to ensure ongoing maintenance of security.
    - Physical protection responsibilities will include asset protection, workplace violence prevention, access control systems, video surveillance, and more.
    - Information protection responsibilities will include network security architecture, network access and monitoring policies, employee education and awareness, and more.
  - Work with executives to prioritize security initiatives and spending based on appropriate risk management and/or financial methodology.
  - Maintain relationships with local, state and federal law enforcement and other related government agencies.
  - Oversee incident response planning as well as the investigation of security breaches, and assist with disciplinary and legal matters associated with such breaches as necessary.
  - Work with outside consultants as appropriate for independent security audits.
  - Review internal audit findings with QHSE to ensure impartiality.
  - Set privacy compliance objectives and oversee the privacy program.
  - Collaborate with CITO to oversee The Company's vendor management program.
- **GRC Manager** is responsible for the day to day work of the Security department. Other responsibilities include:
  - Manage the end-to-end process for SOC 2, ISO 27001 and 27701 (from readiness to obtaining and maintaining)
  - Lead the continuous monitoring, remediation, reporting escalation and resolution of security and compliance issues with appropriate leadership
  - Drive improvements in existing processes and develop innovative and efficient solutions

    - Conduct internal security audits, risk assessments and business impact assessments.
    - Work with business leaders to ensure information security risk findings are reviewed and solutions are implemented.
    - Assess the security qualifications of current and potential vendors.
    - Liaise with relevant parties to commission activities related to contingency planning, business continuity management, and IT disaster recovery.
- **General Counsel** is responsible for maintaining an up-to-date registry of regulatory, statutory, and contractual requirements with a specialized focus on security and privacy.
- The **Executive Security Steering Committee** is comprised of the Managing Directors of applicable business units, the VP Information Security, and the VP of Hosting Systems and Operations, and is responsible for the promotion and application of security standards throughout the organization. The **Committee** reviews risk registers, audit results, and security incidents to ensure corrective action takes place.
- **Senior Management and Directors** are responsible for informing personnel of corporate policies as well as enforcing compliance with applicable policies.
- **Managers at all levels** are responsible for informing personnel of corporate policies as well as enforcing compliance with applicable policies.
- **Human Resources personnel** are responsible for providing applicable corporate policies to new Personnel at orientation or time of hire, determining the appropriate documentation of potential violations of applicable policies, and enforcing compliance with applicable policies.
- **Central IT Operations ("CITO") and Security personnel** are responsible for monitoring systems for misuse, promptly investigating suspicious or unauthorized activity, responding to violations of applicable corporate policies (e.g., removal of unauthorized information), and enforcing compliance with applicable policies.
- **All Personnel** are responsible for adhering to policies, completing annual security training requirements, as well as promptly reporting suspicious activities (as a result of any use of their accounts, logon IDs, passwords, PINs, tokens, or other credentials) to a member of the Information Security team, a member of the Human Resources department, or any person in a management position within The Company. Employees and contractors are required to adhere to applicable security and privacy provisions after termination.

ISO 27001:2013 Control 5.1

Top management shall demonstrate leadership and commitment with respect to the information security management system by:
a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement;

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility

ISO 27001:2013 Control 5.3

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management shall assign the responsibility and authority for:
a) ensuring that the information security management system conforms to the requirements of this International Standard;

b) reporting on the performance of the information security management system to top management.

SOC 2: CC1.2

COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Interested Parties

Name of party	Description and requirements	Owner	Monitoring measures
Sister companies	There are limited quality requirements between in-scope entities and other LTG companies or divisions which are usually driven by collaborative customer projects. In these instances they are treated as a partner organization. Sister companies expect the in-scope entities to comply with its information security obligations under ISO/IEC 27001:2013. This is especially important if the information is transferred between two LTG ISO/IEC 27001:2013 accredited companies.	Product Management, Hosting Operations, Professional Services Management	Standard reporting lines with respect to quality are set up between management, which would ultimately report to and be monitored by the Managing Director. Hosting teams maintain multiple monitoring solutions to identify service availability, performance, vulnerabilities, and potential data breaches. Additionally, customer service representatives meet regularly with their Director who brings any customer issues to management meetings of the Senior Leadership team.
Shareholders	Shareholders expect strong sales, good service, high quality and handling information securely in order to ensure a profitable return on their investment.	Business Unit Managing Director(s)	The Managing Directors and the Group Financial Controller from the LTG Finance team to ensure that the business is run in a manner consistent with the budget agreed upon by the Managing Director(s) and the Group Chief Executive Officer. This includes a monthly review of both revenue and expenses to identify emerging places for concern, develop plans for mitigation and ensure we are delivering maximum value.
Service providers and Data Sub-processors	Service providers are companies like Google, Amazon and Egnyte who are providing essential services incorporated into our processes. Data Sub-processors are entrusted with customer data. Their performance impacts The Company's performance. They are required to comply with applicable information security management practices to assist us in our compliance.	Data Protection Office	Our Data Protection Office, is a cross-functional team comprised of Legal department senior leadership and VP Information Security, who ensures that all third-party service providers meet or exceed applicable information security requirements and that a signed DPA is in place, as applicable.

Regulatory bodies	Regulatory bodies are those such as ISO, the ICO, governments etc. who set laws and regulations that govern how we carry out our business and how we should handle information.	See Corporate Risk Register	These entities have individual owners and monitoring measures, depending on the area of the business affected.
Partner organizations	Partner organizations are organizations we may form a partnership or consortium with in order to provide customers a unique set of functionality only available through a combined partnership.	Decided per service	Standard reporting lines are set up between the Sales or Account Management team member responsible for the partnership and the Technical Leader responsible for the delivery and implementation of the partnership project.
LTG	LTG expects in scope entities to comply with all relevant information security requirements where applicable and deliver strong sales, good service, and high quality so that they may deliver value to shareholders. They also drive the overall business strategy into which the businesses must fit, and create approved operating budgets.	Managing Director(s)	The Managing Director(s) reports to the LTG board on the current state of business and information security.
Employees	Employees expect fair treatment and remuneration, a chance to develop their skills and advance within the organization, and for their information and that of others to be handled, processed and stored securely.	Line managers/HR	Line managers have regular 1-2-1s with their direct reports and can escalate any issue not within their power to resolve to their own line manager. LTG's HR team within Central Ops provide developmental resources such as training in consultation with line managers, including providing line management training and support to new managers.
Customers	Customers are expecting high quality services and goods at a reasonable price, to agreed specifications and for their information to be handled, processed and stored securely.	VP Customer Support and VP Revenue	Account management teams are in regular contact with customers. The VP Customer Support and VP Revenue is part of the The Company's management team and customer service and satisfaction is discussed as part of management meetings. The Company maintains multiple monitoring solutions to identify vulnerabilities and potential data breaches.

ISO 27001:2013 Control 4.2

The organization shall determine:
a) interested parties that are relevant to the information security management system; and
b) the requirements of these interested parties relevant to information security.

ISO 27701:2019 Control 5.2.2

The organization shall include among its interested parties (see ISO/IEC 27001:2013, 4.2), those parties having interests or responsibilities associated with the processing of PII, including the PII principals.
NOTE 1 Other interested parties can include customers (see 4.4), supervisory authorities, other PII controllers, PII processors and their subcontractors.

NOTE 2 Requirements relevant to the processing of PII can be determined by legal and regulatory requirements, by contractual obligations and by self-imposed organizational objectives.

NOTE 3 As an element to demonstrate compliance to the organization's obligations, some interested parties can expect that the organization be in conformity with specific standards, such as the Management System specified in this document, and/or any relevant set of specifications. These parties can call for independently audited compliance to these standards.

SOC 2: CC1.3

COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Legislative Obligations

The Company will ensure that, at all times, its Information Security Management System shall support full compliance with relevant legislation and regulations. The most notable pieces of legislation are:

- The EU General Data Protection Regulation (EU GDPR) 2016/679
- UK General Data Protection Regulation (UK GDPR) 2021
- EU-U.S. Privacy Shield Principles
- Swiss-U.S. Privacy Shield Principles
- The Foreign Corrupt Practices Act (FCPA)
- UK Bribery Act
- Family Educational Rights and Privacy Act
- California Consumer Privacy Act (CCPA - 2020)

The Legal team maintains contract templates giving standard terms and conditions. When a new client engagement is made, these templates are the ones that The Company use. Should the client request any changes to the standard contract, Legal will review the suggested amendments and advise accordingly.

Legal will also review contracts where The Company is the client. With the larger suppliers such as Google and Amazon it may not be possible to make any changes to terms and conditions, but we are still aware of what the contract says. Where feasible, Legal may ask for amendments to be made where required in the case of smaller suppliers.

It is the responsibility of Legal to monitor all changes in the law and advise Group companies accordingly.

The VP Information Security works with Legal to ensure that The Company maintains its Privacy Shield certification on an annual basis.

Contractual Obligations

This table provides a list of common contractual obligations required by client service agreements. Each client service agreement is different but contain obligations such as:

Obligation	Condition
Uptime	The Company's standard Service Level Agreement provides for an annual up time and availability measurements for hosted implementations of it systems.

Backup Frequency	Data backups are performed on a nightly schedule in support of contractual obligations for availability and disaster recovery capabilities.
Content Backup Retention Period	Data retention periods are determined by clients as a part of their implementation and internal management of their data.
Standard Support Response Time	Support response time is governed by the then current version of the The Company Standard Service Level Agreement.
Critical Support Response Time	Support response time is governed by the then current version of the The Company Standard Service Level Agreement.
Audit Trail Retention	Application audit data is maintained indefinitely within each client's implementation, for the duration of the service engagement.
Privacy and Security	The Company will implement appropriate security requirements to protect Personal Data in accordance to requirements the Standard Contractual Clauses.
Software Updates	Updates to The Company software will be made available to client for the duration of the service engagement.
Planned Downtime Notice	Support response time is governed by the then current version of the The Company Standard Service Level Agreement.
Liability Insurance	The Company will maintain active Cyber Insurance coverage for the duration of the service engagement, at appropriate levels for the data it processes.
Business Continuity and Disaster Recovery Plans	The Company will maintain and test its Business Continuity and Disaster Recovery Plans.
Background Screening	The Company employment policies require personnel to undergo background checks.

ISMS Implementation

Objectives

The Company's Information Security and Privacy objectives are derived from its **Mission** (as stated above):

- *to protect the confidentiality, integrity, and availability of the information assets of the company, its partners, and its customers through practices and infrastructure in a way that is aligned with The Company's business goals, risk posture, and ethics*
- *to enable business opportunity by aligning The Company's risk posture and security, privacy and compliance capabilities with the values and requirements of The Company's customers and prospective customers.*

The Company's use of quarterly Internal Audits establishes a baseline for its performance, where any nonconformities that arise are measured, tracked, and resolved to ensure Security and Privacy thresholds are being met. Quarterly Internal Audit results are shared in the Executive Security Steering Committee meetings where NCNs and IRLs are addressed and remediation plans and timelines are developed. The NCMs and IRLs are documented in the Executive Security Steering Committee meeting minutes and are tracked in the Risk Register.

ISO 27001:2013 Control 9.3

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The organization shall retain documented information as evidence of the results of management reviews.

SOC 2: CC2.1

COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Resources

The Company shall identify and make available all the resources (e.g. knowledge, infrastructure, people, work environment, finance, support) required to:

- Implement the ISMS
- Maintain its effectiveness
- Meet regulatory and requirements of the standard
- Provide assurance that the ISMS undergoes a process of continual improvement

Finance

Funding for resources is reassessed annually. Budgets are created during Q4 for the following financial year. Each budget holder is required to submit their budget requirements, which are then reviewed and renegotiated /approved jointly by the LTG Board and Finance teams after considering them against the group and company strategic aims, growth targets, expected revenue figures, etc.

The **Managing Director, LTG board** and **Finance Team** are responsible for setting the overall budget for PeopleFluent.

The **Managing Director** is responsible for planning what resources are required, then creating and submitting their company's budget for approval

The **VPs** and **Directors** are responsible for planning what resources are required, then creating and submitting their teams' budget for approval

People

Evaluation of the currently available employee's capability of supporting core business functionality, the ISMS, and any other additional work is carried out at regular intervals. This process takes place in personnel meetings such as:

- Daily standup meetings for each team, in which the work for the previous day is discussed along with the work for the present day. Any timeline slippage or constraints on current projects are reported to the team lead.
- Weekly departmental meetings, in which department heads meet with the MD to discuss ongoing work. Any timeline slippage or constraints on current projects are reported to the MD.
- Quarterly company meetings, in which a retrospective of work completed and upcoming roadmap items are discussed.

Additional personnel requirements are considered as part of the annual budgeting process, taking into account the anticipated work for the next year and the ability to perform the required work of the current year in a timely manner as indicated by regular personnel meetings.

SOC 2: CC1.5

COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Infrastructure

Buildings, computer hardware and information and communication technology services are the key pieces of infrastructure for The Company. Requirements for new or upgraded infrastructure are considered as part of the budgeting process.

Organizational knowledge

The Company (plus LTG Central Ops and some other LTG brands) use the Atlassian Confluence product, in which this manual resides, as the place to capture organizational knowledge.

All spaces are live and dynamic. Spaces and pages within are considered controlled upon their creation, via the implementation of the inerrant Confluence versioning system plus editing and viewing restrictions applied from the parent Space. Confluence pages that are for

information only, for example, a page discussing upcoming social events, are the exception - these are classified as uncontrolled pages, although the version control and history still remain in place.

Access to, and read/write permissions for, spaces are controlled according to the subject of the space, but for the most part everyone can access every space. If a space held privileged or confidential information, access would be restricted. For example, spaces holding personal information, or information that could affect the share price, are shared only on a need to know basis.

Maintenance of the ISMS

Requirements for management and maintenance of the ISMS are considered in the same way. Annual budgets will include all necessary expenses for industry accreditation, vulnerability management, pen testing, continuing security education, and other expenses deemed necessary by the **VP Information Security**.

ISO 27001:2013 Control 7.1

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

ISMS policies and practices undergo continual updates and improvements to stay abreast of current Security and Privacy concerns as well as issues related to ongoing business operations.

ISO 27001:2013 Control 4.4

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

ISO 27701:2019 Control 5.2.4

When determining the scope of the PIMS, the organization shall include the processing of PII.
NOTE The determination of the scope of the PIMS can require revising the scope of the information security management system, because of the extended interpretation of "information security" according to 5.1.

SOC 2: CC3.4

COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

Competence

The Company shall ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

- Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
- Verification of the applicant's curriculum and confirmation of claimed academic and professional qualifications.
- Identity verification.
- Conduct ongoing evaluations to ensure competencies are aligned with role responsibilities.
- Provide training to ensure policy awareness and maintain correct competency levels.

SOC 2: CC1.4

COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Responsibilities

- The **LTG HR team** are responsible for conducting employment qualification verification checks, the production, distribution, publicizing and monitoring of uptake of mandatory training material (such as Anti-Bribery and Corruption, GDPR Compliance, etc.).

- **All staff members** are responsible for undertaking, completing and successfully passing any completion criteria for mandatory training pieces.
- The **LTG HR team** are responsible for assessing requests for training from The Company to determine the best way to meet the training need, and to assign resources or budget to meet that need.

Staff are employed initially with the highest level of competence and experience available, backed up where required with suitable qualifications. The exception to this is in the case of designated interns, trainees and apprentices who are appointed on the basis of their aptitude and potential. During the hiring process, candidates will have their CV and credentials scrutinized, and then be interviewed by senior personnel within The Company. The Company uses a vendor to conduct background checks on potential applicants.

After an applicant accepts the position, the applicant is required to sign a contractual agreement, acknowledging the terms and conditions of employment.

During onboarding, line managers and team leaders will carry out 1:1 training and mentorship to help them understand The Company's expectations, how our tools work, and so on.

Directors and senior staff may attend industry seminars, conferences and courses to keep abreast of the latest developments and techniques, and pass knowledge and skills gained to other levels of staff via in-house individual training. Specialist skills and training are developed through in-house procedures and training sessions, online resources, on-the-job instructions and via recognized training courses.

Personnel records, including records of career progression and 1-2-1s are held in The Company’s Performance and Learning Management tool.

ISO 27001:2013 Control 7.2

The organization shall:
a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;

d) retain appropriate documented information as evidence of competence. NOTE Applicable actions may include, for example: the provision of training to, the mentoring of, or the re- assignment of current employees; or the hiring or contracting of competent persons.

Awareness

It is the policy of The Company that information about the ISMS, the information security policy, the management objectives, the activities around it and other relevant information be made available to The Company's employees. It should form part of a new starter's induction, it should be reviewed annually and, where information has changed that affects an existing employee, a communications plan exists to update their knowledge.

- **Managers** are responsible for ensuring their employee complete onboarding actions, highlighting The Company’s Information Security and Privacy initiatives and policies.
- The **VP Information Security** is responsible for the creation of the communications plan and assets, for execution of the communications plan, and for keeping Personnel apprised of

Within The Company training around the ISMS takes several forms:

- Initially training and awareness is imparted as part of the induction process
- There are more targeted update and refresher pieces of training around specific topics, e.g. Secure Development Training
- We may also do webinars, team training sessions, etc. around specific topics if they are deemed necessary
- The **VP Information Security** is responsible for ensuring relevant employees complete the training annually following review and updating of the training by the **VP Information Security** and the **HR Team**.

ISO 27001:2013 Control 5.2

Top management shall establish an information security policy that:
a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;
c) includes a commitment to satisfy applicable requirements related to information security; and
d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:
e) be available as documented information;
f) be communicated within the organization; and
g) be available to interested parties, as appropriate.

ISO 27001:2013 Control 7.3

Persons doing work under the organization's control shall be aware of:
a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance;

c) the implications of not conforming with the information security management system requirements.

Communication

All internal and external communications with concerning the ISMS, policy changes, and incident responses should be informative, transparent, and expedient. All communications should only be delivered to impacted parties and should include pertinent details, dates, and actionable items. The goal of ISMS related communications is to deliver the right information to the right parties as soon as possible.

All internal and external communications with concerning the ISMS, policy changes, and incident responses should be reviewed by the **VP Information Security** and **MD**. Communications with external customers will be provided by the **VP Customer Support**, **VP Revenue** or appointed personnel.

SOC 2: CC2.2

COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

SOC 2: CC2.3

COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

Client-specific communications

What?	When	To Whom	How	From Whom
Product Release Notes	Product Release	Public	Client service portal	Product Management
Project milestone status updates	Throughout an active implementation or upgrade project	Client contacts & associated account managers	Client service portal	Services Team

General communications

What?	When	To Whom	How	From Whom
Quarterly ISMS report (covers audit results, NCNs, corrective actions,	Before the quarterly The Company management meeting	The Company management team	Written document, part of the management pack	VP Information Security

reports on internal projects)				
Company updates (financial performance, market updates, news, targets and objectives)	Minimum twice a year, usually January and September/October; may be more common if there is significant news	Whole company	Webinar	MD (or, where presentations must be simultaneous such as in the event of a new acquisition, another member of the management team)
Manager update emails (general central ops and group activity and information, sometimes with actions to managers)	Monthly, or more frequently if circumstances dictate	Line managers across the group	Email	It's compiled by the Internal Learning Consultant
Operational status updates or live collaboration communications for change implementation and hosting systems administration	Live	Hosting Operations and Customer Support Teams	Slack collaboration hub	Hosting, Security, and Support team members
Changes to operations security policies or SOP's.	When approved changes are published.	Hosting Operations Team and other service operations teams.	Confluence	Hosting Team management line and the VP Information Security

In general terms, various communication methods are used to help communicate and achieve business goals. These include, but are not limited to:

- Management meetings and actions
- Confluence
- Emails and presentations from the Management team
- The appraisal cycle
- Ongoing performance reviews and one-to-ones
- Webinars and Hangouts
- Business unit meetings
- Project team meetings
- Cross-team meetings based around a topic or skill set
- Newsletters
- Surveys
- Posters
- Videos

ISO 27001:2013 Control 7.4

The organization shall determine the need for internal and external communications relevant to the information security management system including:
a) on what to communicate;
b) when to communicate;
c) with whom to communicate;
d) who shall communicate; and
e) the processes by which communication shall be effected.

Documentation

The Company's policy around documented information is twofold:

- Where documents need to be created, they should be created from a controlled and maintained document template stored within a central register within Confluence
- Following an Agile mindset, documents should only be created where there is a clear need and where they create value

It is the responsibility of **managers** in charge of processes to advise the **VP Information Security** when new document templates or content have been created or updated, and provide this to them for controlling.

The **VP Information Security** is responsible for ensuring templates are checked, versioned correctly, and uploaded to the appropriate location in Confluence.

ISMS documents

ISMS policies are only available via Confluence. The VP Information Security is responsible for ensuring that these documents reflect The Company's requirements and practices, and that amendments are instituted in a timely manner.

ISMS policies are to be reviewed *at least* annually. This review is stated in each policy's **Document Control** and **Version History**

Record control

Electronic records of audits, inspections, feedback data and issues are held indefinitely. Sensitive data such as client or personally identifiable information (PII) will be retained according to legal requirements. See also: Data Classification and Handling Policy

ISO 27001:2013 Control 7.5.1

When creating and updating documented information the organization shall ensure appropriate:
a) identification and description (e.g. a title, date, author, or reference number);
b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
c) review and approval for suitability and adequacy.

ISO 27001:2013 Control 7.5.2

Documented information required by the information security management system and by this International Standard shall be controlled to ensure:
a) it is available and suitable for use, where and when it is needed; and
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:
c) distribution, access, retrieval and use;
d) storage and preservation, including the preservation of legibility;
e) control of changes (e.g. version control); and
f) retention and disposition.
Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

ISO 27001:2013 Control 7.5.3

Documented information required by the information security management system and by this International Standard shall be controlled to ensure:
a) it is available and suitable for use, where and when it is needed; and
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:
c) distribution, access, retrieval and use;
d) storage and preservation, including the preservation of legibility;
e) control of changes (e.g. version control); and

f) retention and disposition.
Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the

Security Documentation Overview .

Document control

This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado	
Author(s)	@Art Machado @Sarah Zwicker (Unlicensed) @John Cole	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Mar 12, 2024
Review cycle	ANNUAL	
Next review date	Mar 12, 2025	

Version History

Date	Author(s)	Version	Changes
Nov 1, 2024	@angelina.kilmer	3.7	Changed Policy classification from Confidential to Public
Mar 12, 2024	@Sarah Zwicker (Unlicensed) & @Art Machado	3.6	Annual review + Legal Entity change
Feb 23, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	3.5	Annual review + logo change
Nov 15, 2022	@Sarah Zwicker (Unlicensed)	3.4	Removed references to CTO.
Apr 14, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	3.3	Changed Scope statement to incorporate Privacy (ISO 27701) adding more privacy considerations; Added Objectives section;

Mar 16, 2022	@Art Machado & @Sarah Zwicker (Unlicensed)	3.2	Title Changes and Annual Review
May 6, 2021	@Sarah Zwicker (Unlicensed) & @Art Machado	3.1	Changed Scope statement per ISO non-conformity
Mar 9, 2021	@Sarah Zwicker (Unlicensed)	3.0	Changed owner, updated Security Statement and Overview
Feb 9, 2021	@Sarah Zwicker (Unlicensed)	2.9	Reformatting, linked policies
Jan 26, 2021	@John Cole	2.8	Annual review, role title change
Nov 23, 2020	@Sarah Zwicker (Unlicensed)	2.7	Changed Owner and addition of supplemental security policy for legacy NetDimensions hosting operations, PF-ISMS-0015