Information Security Statement

Version number	5.0
Last Approved	Feb 13, 2026
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.

Scope

This statement applies to any electronic information storage or physical media containing sensitive or confidential data stored or processed by The Company or its trusted subcontractors.

ISO 27001:2022 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.

ISO 42001:2023 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 result(s) of its AI management system.

The organization shall consider the intended purpose of the AI systems that are developed, provided or used by the organization. The organization shall determine its roles with respect to these AI systems.

Information Security Statement

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

Scope of the ISMS

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;
- Hosting Operations and Security for all applicable SaaS offering systems and product lines. The Company’s security policies apply equally to all cloud-based, hybrid, and data center operations;
- Documentation, communication, performance and continuous improvement of these governance processes.

ISO 27001:2022 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.

ISO 42001:2023 Control 4.3

The organization shall determine:

> *— the interested parties that are relevant to the AI management system;*
>
> *— the relevant requirements of these interested parties;*
>
> *— which of these requirements will be addressed through the AI management system.*

Objectives

The Company's Information Security and Privacy objectives are derived from its **Mission** and **Strategy**:

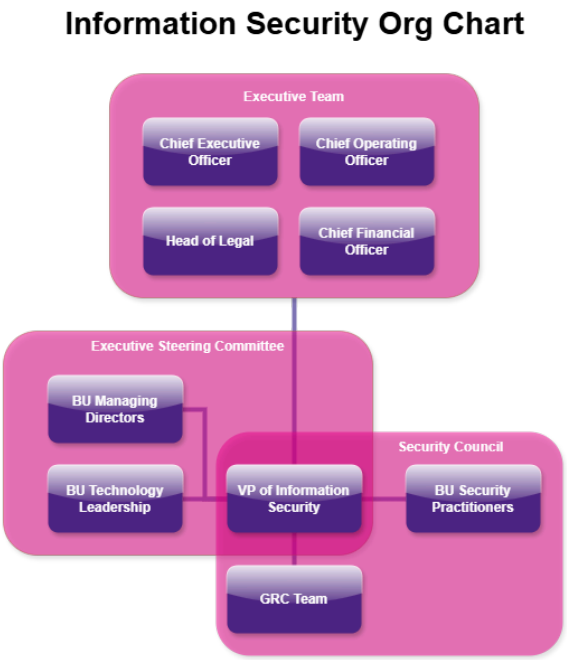
- *The Company's Information Security Mission is:*
  - *to protect the confidentiality, integrity, and availability of the information assets of the company, its partners, and its customers through practices and infrastructure in a way that is aligned with The Company's business goals, risk posture, 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 priorities.*

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 Org Chart below denotes the security reporting lines and the scope of collaborative groups such as the Security Council.



The following outlines additional role-specific responsibilities:

VP Information Security

The VP Information Security is responsible for oversight of security and privacy and establishing the appropriate processes and capabilities to ensure compliance with all relevant security and privacy commitments. The VP of Information Security ensures that effective organizational structures and policies are in place within the Company to drive, support, and monitor the performance of the security and privacy programs and the fulfilment of the security and privacy mission and objectives.

GRC team

The team is overseen by the VP of Information Security. Their remit is to execute the security and privacy related tasks that underpin the responsibilities of the VP of Information Security to ensure compliance with required standards.

Some of these tasks include but not limited to conducting internal audits, prepare and gather evidence for external audits, manage the processes for vendor review, offboarding, risk assessment and business continuity.

Central Operations teams

Legal are responsible for maintaining an up-to-date registry of regulatory, statutory, and contractual requirements with a specialized focus on security and privacy.

The **People team** are responsible for providing applicable corporate policies to new Personnel at orientation or time of hire, conducting background checks on all new hires, oversee the performance management conversations and ensure employee compliance with mandatory training requirements.

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.

The Executive Steering Committee

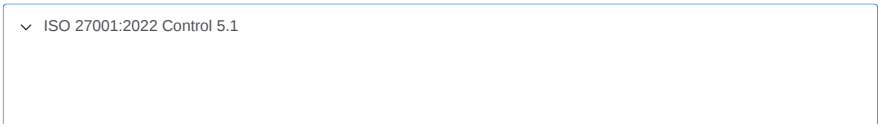
The Executive Security Steering Committee is comprised of the Managing Directors of applicable business units, the VP Information Security, and relevant leadership roles from the BUs, and is responsible for the promotion and application of security standards throughout the organization. The Committee reviews risk registers, audit results, and security incidents to ensure corrective action takes place.

Security Council

The Company's Security Council is comprised of technical security leaders from the Company's various business units. The Council meets monthly and serves as the primary mechanism to establish and ensure the uniform implementation of the Company's security standards across the business.

All Personnel

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 People team, 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.



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 27001:2022 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.

ISO 42001:2023 Control 5.1

Top management shall demonstrate leadership and commitment with respect to the AI management system by:

— ensuring that the AI policy (see 5.2) and AI objectives (see 6.2) are established and are compatible with the strategic direction of the organization;

— ensuring the integration of the AI management system requirements into the organization's business processes;

— ensuring that the resources needed for the AI management system are available;

— communicating the importance of effective AI management and of conforming to the AI management system requirements;

— ensuring that the AI management system achieves its intended result(s);

— directing and supporting persons to contribute to the effectiveness of the AI management system;

— promoting continual improvement;

— supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.

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
Service providers and Data Sub-processors	Service providers are companies who are providing essential services that support the companies' processes. Their performance impacts The Company's performance. They are required to comply with applicable information security management practices to assist us in our compliance.	GRC Team	Appropriate Vendor & Privacy Management processes are in place to ensure alignment with all relevant laws and regulations, and organizational commitments and interests.
Regulatory bodies	Regulatory bodies are those such as the ICO and other governmental data protection agencies who set laws and regulations which stipulate requirements for how we conduct our business and process data.	Legal Team	Processes in place to track and monitor all legal and regulatory requirements to effectively communicate such requirements and monitor compliance throughout the business.
Employees	The Company processes Employee personal data and relies on employees to fulfill critical roles in supporting the ISMS.	People Team	Onboarding, training, performance management, and

			privacy management processes in place.
Customers	Customers are expecting their information to be handled, processed and stored securely.	VP of Information Security	Our internal and external audit program is designed to ensure we meet all client security requirements

ISO 27001:2022 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 27001:2022, 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.

ISO 42001:2023 Control 4.2

The organization shall determine:

— the interested parties that are relevant to the AI management system;

— the relevant requirements of these interested parties;

— which of these requirements will be addressed through the AI management system.

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 is committed to complying with relevant laws and regulations applicable to its business. The Information Security Management System and Privacy Information Management System have been structured with key legislation pertinent to the Company's operations in mind, including data protection regulations and anti-bribery and corruption laws. The Company will periodically monitor changes in key legislation and evaluate whether modifications or updates to its Information Security Management System are required.

Contractual Obligations

Contractual obligations are used to provide assurance to customers and other sub-service providers such as sub-processors. Obligations may vary depending on the BU and or the product or service however some common examples include:

- SLAs
- Updates and patching
- Backup frequency
- Audit trail retention
- Privacy

Our audit program is designed to ensure that contractual obligations are faithfully met via the ISMS and PIMS.

ISMS Implementation

The Company's use of 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. Internal Audit results are shared in the Executive Steering Committee and Security Council meetings where issues are addressed and remediation plans and timelines are developed.

ISO 27001:2022 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 results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

SOC 2: CC2.1

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

ISO 42001:2023 Control 9.3

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

The management review shall include:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the AI management system;

c) changes in needs and expectations of interested parties that are relevant to the AI management system;

d) information on the AI management system performance, including trends in:

1. *nonconformities and corrective actions;*
2. *monitoring and measurement results;*
3. *audit results;*

e) opportunities for continual improvement.

The results of the management review shall include decisions related to continual improvement opportunities and any need for changes to the AI management system.
Documented information shall be available as evidence of the results of management reviews.

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 and PIMS
- Maintain its effectiveness
- Meet regulatory and requirements of the Standards
- Provide assurance that the ISMS and PIMS undergo a process of continuous improvement

Finance

Annual budget assessments consider ISMS and PIMS requirements and ensure appropriate allocation of resources to support critical processes.

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 captures organizational knowledge within our intranet, allowing us to ensure that appropriate access to organizational knowledge is available to everyone in scope

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.

Maintenance of the ISMS

Annual budgets will include all necessary expenses for industry accreditation, vulnerability management, pen testing, continuing security education, and other expenses deemed necessary.

ISO 27001:2022 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 and PIMS 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 27001:2022 Control 4.4

The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

ISO 42001:2023 Control 4.3

The organization shall establish, implement, maintain, continually improve and document an AI management system, including the processes needed and their interactions, in accordance with the requirements of this document.

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 ensures 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
- Verification of the applicant's claimed academic and professional qualifications
- Conduct ongoing performance reviews to ensure competencies are aligned with role responsibilities
- Provide training to ensure policy awareness and maintain correct competency levels
- All Personnel are contractually committed to comply with all applicable security, confidentiality, and privacy requirements as well as with the Company's broader policies and Code of Conduct

SOC 2: CC1.4

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

SOC 2: CC1.5

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

ISO 27001:2022 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.

ISO 42001:2023 Control 7.2

The organization shall:

— determine the necessary competence of person(s) doing work under its control that affects its AI performance;

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

— where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken.

Appropriate documented information shall be available as evidence of competence.

Responsibilities

- The **People team** are responsible for conducting employment qualification verification checks, and compliance training.
- **All staff members** are responsible for undertaking, completing and successfully passing any completion criteria for mandatory training pieces.

Awareness

It is the policy of The Company that information about the ISMS, the information security and privacy policies, the management objectives, the activities around it and other relevant information be made available to The Company's personnel. It forms part of a new starter's induction and is reviewed at least annually.

- **Managers** are responsible for ensuring their employee complete onboarding actions, highlighting The Company's Information Security and Privacy initiatives and policies.

ISO 27001:2022 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 27001:2022 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.

ISO 42001:2023 Control 5.2

Top management shall establish an AI policy that:

a) is appropriate to the purpose of the organization;

b) provides a framework for setting AI objectives (see 6.2);

c) includes a commitment to meet applicable requirements;

d) includes a commitment to continual improvement of the AI management system.

The AI policy shall:

— be available as documented information;

— refer as relevant to other organizational policies;

— be communicated within the organization;

— be available to interested parties, as appropriate.

Communication

Communications must consider:

- **What** is communicated
- **When** to communicate
- **To who** should we communicate with

- **How** should we communicate
- **From who** should communications be sent

Communications must be compliant with the Data Classification and Handling Policy

ISO 27001:2022 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) how to communicate.

ISO 42001:2023 Control 7.4

The organization shall determine the internal and external communications relevant to the AI management system including:
— what it will communicate;
— when to communicate;
— with whom to communicate;
— how to communicate.

SOC 2: CC2.3

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

Documentation

ISMS, PIMS and Related Documents

All formalized policy documentation is centrally stored and managed within a Global Policy Register published on the Company's intranet, which is communicated to and available to all Employees.

Record control

All formalized policy documentation includes record control / change logs and undergoes formalized review and approval at least annually.

As with all Company information, ISMS and PIMS documentation complies with the Company's Data Classification and Handling Policy and Data Retention, Destruction and Disposal Policy

ISO 27001:2022 Control 7.5.1

The organization's information security management system shall include:
a) documented information required by this document; and
b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE The extend of the documented information for an information security management system can differ from one organization to

another due to:
1) the size of the organization and its type of activities, processes, products and services;
2) the complexity of processes and their interactions; and
3) the competence of persons.

ISO 27001:2022 Control 7.5.2

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 27001:2022 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.

ISO 42001:2023 Control 7.5.1

The organization's AI management system shall include:

a) documented information required by this document;

b) documented information determined by the organization as being necessary for the effectiveness of the AI management system.

NOTE The extent of documented information for an AI management system can differ from one organization to another due to:
— the size of organization and its type of activities, processes, products and services;

— the complexity of processes and their interactions;
— the competence of persons.

ISO 42001:2023 Control 7.5.2

When creating and updating documented information, the organization shall ensure appropriate:

— identification and description (e.g. a title, date, author or reference number);

— format (e.g. language, software version, graphics) and media (e.g. paper, electronic);

— review and approval for suitability and adequacy.

ISO 42001:2023 Control 7.5.3

Documented information required by the AI management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;

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:

— distribution, access, retrieval and use;

— storage and preservation, including preservation of legibility;

— control of changes (e.g. version control);

— retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the AI management system shall be identified as appropriate and controlled.

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, Angelina Kilmer, Paul Gordon	
Required Approver(s) and Approval Date	Art Machado - VP Information Security	Feb 13, 2026
Review cycle	ANNUAL	

Next review date	Feb 12, 2027

Version History

Date	Author(s)	Version	Changes
Feb 13, 2026	Angelina Kilmer, Paul Gordon	5.0	Annual review
Jan 22, 2026	Art Machado, Angelina Kilmer, Paul Gordon	4.4	ISMS applies equally to cloud-based, hybrid, and data center operations
Apr 24, 2025	Art Machado, Angelina Kilmer, Paul Gordon	4.3	Updated Org Chart including roles & responsibilities, revised list of relevant Interested, and streamlined communication & documentation sections
Apr 9, 2025	Paul Gordon	4.2	References to ISO 42001
Apr 1, 2025	Paul Gordon	4.1	Updated references from 2013 standard to 2022
Feb 25, 2025	Art Machado, Angelina Kilmer, Paul Gordon	4.0	Annual review
Nov 1, 2024	Angelina Kilmer	3.7	Changed Policy classification from Confidential to Public
Mar 12, 2024	Art Machado, Sarah Zwicker	3.6	Annual review + Legal Entity change
Feb 23, 2023	Art Machado, Sarah Zwicker	3.5	Annual review + logo change
Nov 15, 2022	Sarah Zwicker	3.4	Removed references to CTO.
Apr 14, 2022	Art Machado, Sarah Zwicker	3.3	Changed Scope statement to incorporate Privacy (ISO 27701) adding more privacy considerations; Added Objectives section;

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