Information Security Policy

Purpose

Argo Group International Holdings, Ltd. ("Argo Group") has established this Information Security Policy to set out the information security requirements and expectations to which employees, third parties, processes and adopted technology solutions must comply.

This policy demonstrates Argo Group commitment to protecting information, systems and people across the enterprise. Information is a critical and essential asset to Argo Group and maintaining confidentiality, integrity and availability is necessary to maintain business operations and regulatory compliance.

Scope

This Information Security Policy and related framework is applicable to:

- all information assets and systems that are owned and operated by Argo Group,
- third parties acting on behalf of Argo Group or processing Argo Group information,
- Argo Group business processes,
- Argo Group employees and contractors.

The scope may be expanded or adjusted at any time based on identified risks and/or at the request of the Argo Group Security Governance Council (the "SGC").

Compliance and Review

All in scope components must comply with this policy and the supporting standards.

If adherence to this policy and supporting standards cannot be reasonably achieved, an exception may be granted subject to evaluation and acceptance of the risk presented. The evaluation must articulate the impact to the ISP objectives.

In scope employees and/or Third-Parties who fail to comply with this policy and related standards are subject to the Argo Group disciplinary process or applicable contractual provisions.

To ensure continuing suitability, adequacy and effectiveness, Argo Group will review information security policies and standards on an annual basis.

References and Framework

Information security activities at Argo Group were originally developed based on the standard National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) version 1.1, and applicable legal and/or regulatory requirements.

Roles and Responsibilities

Security Governance Council is responsible for;

- Providing management oversight and executing responsibilities as per the Security Governance Council Charter.

Chief Administrative Officer (“CAO”) is responsible for;

- Acting as the executive sponsor for the information security and data protection programs;
- Providing administrative support to the Security Governance Council.

Chief Security Officer (“CSO”) is responsible for;

- Overseeing the implementation and enforcement of the company’s information security program;
- Ensuring an appropriate level of protection for Argo Group information resources;
- Setting, monitoring and reporting of information security objectives.
- Reporting from time to time to the Board of Directors for each Argo Group entity.

General Counsel (“GC”) is responsible for;

- Providing guidance and direction regarding legal and/or regulatory compliance requirements and works with law enforcement or regulatory authorities in the event of an information security incident with a material business impact;

Chief Risk Officer (“CRO”) is responsible for;

- Managing corporate cyber liability insurance placement and loss reporting;
- Operating the Enterprise Risk Management program which considers information security and data protection risks

Company Management is responsible for;

- Supporting the implementation of this policy and related standards within the business areas for which they are responsible;
- Making the necessary time and resources available to adopt secure working practices within their function.

Users (employees and contractors) are responsible for;

- Complying with this ISP and other adjacent policies, procedures, application regulations and laws;
- Reporting violations of this ISP to their supervisor or manager;

External Partners are responsible for;

- Consistently respecting and protecting the privacy and confidentiality of the information they have access to;
- Complying with contractual provisions;
- Reporting potential and actual security incidents to Argo Group when they are identified;

Policy Objectives

A principal set of policy objectives has been established to provide direction and structure to the information security program. These objectives are reviewed and updated from time to time and approved by the Security Governance Council.

Argo Group has established and will maintain a set of standards to enable the achievement of these objectives.

Management Commitment and Oversight

Objective: Operate a management framework providing direction and oversight for information security in accordance with business requirements, relevant laws and regulations.

Supporting Policies and Standards:	***Reference:***
Argo Group Information Security Policy (This Policy)	*All Sections*
Argo Group Security Governance Council Charter	*All Sections*
Argo Group Minimum Information Security Standards	*ID.GV*

Risk Management

Objective: Argo shall establish a capability to identify and manage enterprise, operational and technical security risks within its business environment.

Supporting Policies and Standards:	***Reference:***
Argo Group Risk Management Policy	*All Sections*
Argo Group Risk Management Framework	*All Sections*
Argo Group Minimum Information Security Standards	*ID.RM, ID.RA*

Incident Response

Objective: Argo shall maintain a Security Incident Response Plan to ensure adequate response and recovery to security events.

Supporting Policies and Standards:	***Reference:***
Argo Group Incident Response Plan	*All Sections*
Argo Group Minimum Information Security Standards	*RS.RP*

Third Party Management

Objective: Argo shall deploy adequate protections where third party and supply chain relationships introduce security risks and vulnerabilities to the organization.

Supporting Policies and Standards:	***Reference:***
Argo Global Group Vendor Management Policy	*All Sections*
Argo Group Minimum Information Security Standards	*ID.SC*

Access Control and Identity Management

Objective: Argo shall ensure that physical and logical access to information, systems and facilities is adequately controlled to prevent business interruption, data breaches and fraud.

Supporting Policies and Standards:	***Reference:***
Argo Group Access Control Standard	*All Sections*
Argo Group Physical Access Control Review Standard	*All Sections*
Argo Group Secure Working Environment Standard	*All Sections*
Argo Group Minimum Information Security Standards	*PR.AC*

Data Protection

Objective: A data protection program will be established and maintained to address regulatory requirements and manage risk as it relates to data.

Supporting Policies and Standards:	***Reference:***
Argo Group Data Protection Framework	*All Sections*
Records and Information Management Policy	*All Sections*
Argo Group Privacy Policy	*All Sections*

Training, Awareness and Competence

Objective: Argo shall ensure that employees and third parties maintain sufficient levels of security awareness and competence as relevant to their job function or contractual agreement.

Supporting Policies and Standards:	***Reference:***
Argo Group Minimum Information Security Standards	*PR.AT*

Minimum Security Standards

Objective: Minimum security standards will be established, documented and communicated to employees and third parties.

Supporting Policies and Standards:	***Reference:***
Argo Group Minimum Information Security Standards	*All Sections*

Technical Controls and IT Security

Objective: Technical capabilities shall be established and maintained to address threats and vulnerabilities within the Argo IT environment.

Supporting Policies and Standards:	***Reference:***
Security Engineering and Architecture Information Protection	*Protections and Controls*
Argo Group Minimum Information Security Standards	*PR.IP*

Compliance

Objective: Argo shall maintain and monitor compliance with standards established to address risks and meet legal/regulatory requirements.

Supporting Policies and Standards:	***Reference:***
Internal Controls Policy	*All Sections*
Argo Group Code of Conduct & Business Ethics	*All Sections*
Argo Group Minimum Information Security Standards	*ID.GV*
Argo Group Internal Audit Policy	*All Sections*
Legal Requirements Register	*All Sections*

Document Control

Ownership:

Policy Owner(s)
Chief Security Officer

Version Control and History:

Version:	Effective Date:	Description	Reviewed and revised by:
V7.0	1st Dec 2021	Policy re-write: Removed ‘standards’ and migrated to ‘Argo Minimum Information Security Standards’. Added policy objectives and updated responsibilities.	Chief Security Officer
V7.0	1st Dec 2021	Policy reviewed Nov 17th 2022 – no significant changes.	Chief Security Officer and Data Protection Officer

Document Governance:

Implementation	
Approved by:	Security Governance Council
Approval Date:	2nd December 2022
Approval Record:	Meeting Minutes – Q4 Security Governance Council