



**SAI360**

ISMS Documentation List



# Confidentiality Statement

This document and any links or attachments may contain copyright material of SAI360 (“SAI360 Inc.”) and/or information that is confidential and subject to privilege. If you are not the intended recipient of this document, please contact SAI360 immediately. In this case, you must not read, print, disseminate, copy, store, or act in reliance on this document or any of the accompanying attachments; and you must destroy all copies of this document. This notice should not be removed.

## Overview

As part of ISO 27001 compliance, SAI360 maintains a set of policies, standards, guidelines, and procedures that include all controls in place related to its information risk management processes.

This document lists SAI360’s Information Security Management System (ISMS) documents, including documents that are mandatory by the ISO 27001:2013 Standard.

SAI360 considers its Policies, Procedures and Standards as confidential intellectual property and in some instances external access would pose a significant risk to our information security. As such we limit the availability of such documents directly to customers. SAI360 will allow customers and or the Independent Auditors of our current customers to view in full relevant Information Security Management System (ISMS) documentation on request either on SAI360 site, or via an Online Meeting screen share or 'Read Only' access via SAI360 SharePoint for nominated personnel for a limited period under a Non-Disclosure Agreement (NDA) or existing Customer Agreement Confidentiality Clause(s).



The following make up SAI360 ISMS documentation:

Document Number	Document Name
ISMS00001	ISMS Documents Architecture
ISMS04001	ISMS Scope
ISMS04002	Information Security Context and Requirements
ISMS05001	Information Security ISMS Policy
ISMS05002	Information Security Roles Responsibilities and Authorities
ISMS06001	Information Security Risk Assessment and Treatment Methodology
ISMS06004	Statement of Applicability
ISMS06002	Risk Assessment and Treatment Sheet.
ISMS06003	Risk Assessment and Treatment Report
ISMS06004	Statement of Applicability
ISMS07002	Procedure for the Control of Documented Information
ISMS07004	Information Security Communication Plan
ISMS09002	Information Security Management System Audit Plan
ISMS09005	Process for Monitoring, Measurement, Analysis and Evaluation
ISMS10002	Nonconformity Management and Continuous Improvement Procedure
ISMS11001	Information Security Policy
ISMS11002	Acceptable Use Policy – Technology
ISMS11003	Data Protection Policy
ISMS11004	End User & Device Security Policy
ISMS12006	Segregation of Duties Guidelines
ISMS13001	Human Resource Security Policy
ISMS13002	Photo ID Policy
ISMS14001	Information Classification and Asset Management Policy
ISMS14002	Information Security Classification Standards
ISMS14004	Procedure for the Management of Removable Media
ISMS14006	Procedure for the Disposal of Media
ISMS14008	IT Equipment Purchasing Policy
ISMS15001	Access Control Policy
ISMS15002	Access Control Standard
ISMS15003	Physical Security Standards
ISMS15005	User Access Management Procedure
ISMS16006	Cryptography Lifecycle Management Standard
ISMS17001	Physical Security Policy
ISMS17008	General Office Infrastructure Design Standard
ISMS18000	Operations Security Management Policy
ISMS18001	Backup and Restore Policy
ISMS18002	Global Naming Standard
ISMS18001	Backup and Restore Policy



ISMS18003	Logging Standard
ISMS18007	Software Policy
ISMS18008	Desktop Security Standard
ISMS18009	Server Security Standards
ISMS18017	Vulnerability Management Standard
ISMS18018	Penetration Testing Methodology and Reporting Guidelines
ISMS18019	Data Leakage Protection Policy
ISMS19005	Network Security Policy
ISMS19006	Network Security Standards
ISMS20009	Secure Development Policy
ISMS20010	Merger and Acquisition Assessment
ISMS21001	Supplier Security Management Policy
ISMS21002	Supplier Management Standards
ISMS21003	Supplier Review Guidelines
ISMS22001	Information Systems Incident Management Policy
ISMS22002	Information Security Incident Management Standard
ISMS22003	Information Security Incident Handling Guidelines
ISMS23011	Corporate IT Business Continuity Management Standard
ISMS23012	Business Continuity Management Policy
ISMS23013	Crisis Management Plan
ISMS24001	Information Security Statutory Compliance Policy
ISMS24004	Records Retention and Protection Policy
ISMS24005	Disposition of Customer Confidential Data
ISMS24011	Data Subject Consent and Request Procedure