AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

1 PURPOSE

This manual defines how the Information Security Management System (ISMS) will be set up, managed, measured, reported on and continually improved within NetGain Systems Pte Ltd.

The purpose of the ISMS is to:

- Understand the organisation's needs and the necessity for establishing information security policies and objectives;
- Implement and operate controls and measures for managing the organisation's overall capability to manage information security incidents;
- Monitor and review the performance and effectiveness of information security controls; and
- Continually improve the organisation's information security performance based on objective measurement.

2 REFERENCE

This ISMS basically references the requirements presented in the International Standard ISO/IEC 27001, and adheres to related laws and regulations enacted by the Government of Singapore, any applicable jurisdiction-specific requirements (e.g., in Malaysia), and general administrative policies of the organization.

3 TERMS & DEFINITIONS

Audit	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled
Availability	Information is accessible and usable on demand by an authorised user
Competence	Ability to apply knowledge, experience and skills to achieve intended results
Confidentiality	Information is not made available or disclosed to unauthorised individuals, entities, or processes
Conformity	Fulfilment of a requirement
Control	Measure that is modifying risk
Information security	Preservation of confidentiality, integrity and availability of information
Information security event	Identified occurrence of a system, service or network state indicating a possible breach of information security policies or failure of controls, or a previously unknown situation that can be information security-relevant
Information security incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Information system	Set of applications, services, information technology assets, or other information-handling components
Integrity	Information is appropriate and complete

Objective	Result to be achieved
Organisation	Refers to NetGain Systems Pte Ltd
Outsource	Arrangement where an external party performs part of an organisation's function or process
Policy	Intentions and direction of an organisation, as formally expressed by its top management
Process	Set of interrelated or interacting activities which transforms inputs into outputs
Risk	Effect of uncertainty on objectives
Threat	Potential cause of an unwanted incident, which can result in harm to a system or organisation
Top management	Person or group of people who directs and controls an organisation at the highest level.
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats

4 CONTEXT OF THE ORGANISATION

4.1 Understanding of the Organisation and Its Context

Founded in 2002 and headquartered in Singapore, NetGain Systems is an innovative leader in AI Ops for IT, specializing in monitoring, observability, and infrastructure management.

With regard to the internal and external environment in which the company operates, there are a number of internal and external issues that the company is facing or may face that may be relevant to the ISMS:

INTERNAL ISSUES	EXTERNAL ISSUES
• Governance, organisational structure and potential changes • Information security culture, standards and processes adopted • Skill sets in software products and services • Available resources • Technology and infrastructure • Relationships with suppliers and customers • Revenue streams and cost structure	• Industry trends and customer preferences • Competition • Laws and regulations and potential changes including those related to information security and privacy • Technological trends and innovations • Cybersecurity threats • Economic factors e.g., lack of customer demand, recession • Force majeure events where the Company has no control of such as acts of God, act of war, action by government, pandemics, natural events, climate change and other disruptive events

The above issues will be considered in determining risks and opportunities and will be monitored during regular information security meetings and/or management review to incorporate any significant changes and to cater for the implications of such changes.

4.2 Understanding the Needs and Expectations of Interested Parties

Interested parties that may be relevant to ISMS and their requirements including the determination of which of these requirements can be addressed by the ISMS are detailed below:

INTERESTED PARTIES (INTERNAL/EXTERNAL) AND THEIR REQUIREMENTS		Can be addressed through the ISMS?	
		Yes	No
Management	• Organisational reputation, growth and profitability • Governance and compliance with organisational policies, procedures and controls including those related to information security and data protection • Compliance with applicable laws, regulations, contractual obligations	√ (indirectly but with impact) √ √	
Employees	• Availability of resources, clear policies, procedures and control measures • Effective communication channels • Personal data protection • Job security, safe and conducive working environment	√ √ √	√
Suppliers	• Clear scope of contractual relationships including those related to information security and data protection • Compliance with applicable laws and regulations and adherence to contractual obligations • Data security • Undisruptive services	√ √ √ √	
Clients	• Meeting contractual requirements • Compliance with client's IT security policies, standards and	√ √	

INTERESTED PARTIES (INTERNAL/EXTERNAL) AND THEIR REQUIREMENTS		Can be addressed through the ISMS?	
		Yes	No
	any instructions on security matters that may be issued by the client subsequently • Access to service should not be affected • Responsiveness and timely resolution of issues • Personal data protection	√ √ √	
Regulatory Bodies / Government Agencies	• Compliance status • Timely notification or submission of required / requested information	√ √	
Emergency Services	• Prompt response and availability	√ (in relation to information security / data breach)	
International Accreditation Forum (IAF) & International Organisation for Standardisation (ISO)	• Address the need to consider the effect of climate change on the ability to achieve the intended results of the management system	√ (indirectly but with impact in relation to the organization's use of virtual machines and serverless computing to reduce hardware resource utilization, and embracing remote work	

The above interested parties and their requirements will be monitored during regular information security meetings and/or management review, and will be considered in determining risks and opportunities.

4.3 Scope of the ISMS

The defined scope of the organisation's ISMS takes into account the internal and external factors, and interested parties and their requirements, as described in sections 4.1 and 4.2.

The scope is defined below in terms of key products and services, physical location, organisation functions and any exclusions.

4.3.1 Products and Services

The following products and services are within the scope of the ISMS:

- ***Provision of IT Observability and Security Management Solutions***

4.3.2 Location

The following offices are within the scope of the ISMS:

- 30 Prinsep Street #06-101, Singapore 188647

4.3.3 Organisation Functions

All the functions reflected in the company's organisation structure are within the scope of the ISMS *(refer to the Company's latest organisation chart).*

4.3.4 Exclusions

To avoid any ambiguity in terms of the scope, the following areas are excluded from the ISMS scope:

- *Processes and infrastructures owned by external parties (e.g., clients, suppliers) which are not under our organisation's control.*
- *Overseas offices (however, all our employees regardless of locations are expected to adhere to all applicable ISMS policies and procedures).*

4.4 Information Security Management System

The organisation is committed to implementing and continually improving our ISMS, including our processes and their interactions, in accordance with the ISO/IEC 27001 Standard. All applicable requirements of the said standard are addressed as indicated in Appendix A.

5 LEADERSHIP

5.1 Leadership and Commitment

The organisation's top management demonstrates leadership and commitment with respect to the ISMS by:

- Ensuring that policies and objectives are established and are compatible with the strategic direction of the organisation;
- Ensuring the integration of the ISMS requirements into the business processes;
- Ensuring that the resources needed for the ISMS are available;
- Communicating the importance of effective ISMS and conforming to the requirements;
- Ensuring that the ISMS achieves its intended outcomes;
- Directing and supporting persons to contribute to its effectiveness;
- Promoting continual improvement;
- Supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility; and
- Involvement through participating in information security meetings e.g., management reviews.

5.2 Policy

The top management has the responsibility to establish an information security management policy, which is aligned with the organisation's strategic direction and provides a framework for setting information security objectives, including a commitment to fulfil applicable requirements and the continual improvement of the ISMS.

The organisation's overarching policy for information security is set out in Appendix B and supported by topic-specific policies as documented in *ISMS-ORG-01 Topic-specific Policies for Information Security*. The said policies are endorsed by the top management and reviewed when significant changes occur or during the yearly management review meeting. The review should ensure that changed requirements and relevant feedback from process owners and other relevant interested parties are considered.

This policy, and any relevant supporting policies, shall be communicated to the appropriate audience, both within and external to the organisation.

5.3 Organisational Roles, Responsibilities and Authorities

Responsibilities and authorities for relevant information security roles are assigned and communicated within the organisation, including those for:

- Ensuring that the ISMS conforms to the requirements of the ISO 27001 Standard; and
- Reporting on the performance of the ISMS to top management.

Details of information security related responsibilities associated with each of the roles and how they are allocated within the organisation are discussed further in *ISMS-ORG-02 Information Security Roles & Segregation of Duties.*

6 PLANNING

6.1 Risks and Opportunities

The organisation plans actions to handle risks and opportunities relevant to its context and the needs and expectations of interested parties. These actions must consider their integration with ISMS activities, as well as how effectiveness should be evaluated.

The identified risks and opportunities, and the action plans, responsibilities and timelines to address them are detailed in Appendix C.

6.1.1 Information Security Risk Assessment

The organisation shall establish, implement and maintain a formal and documented evaluation process for information security risk assessment that:

a) Establish and maintain information security risk criteria that include:
    1) The risk acceptance criteria; and

2) Criteria for performing information security risk assessments

b) Ensures that repeated information security risk assessments produce consistent, valid and comparable results

c) Identifies the information security risks
   1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability within the scope of the ISMS
   2) identify the risk owners

d) analyses the information security risks
   1) assess the potential consequences for the organisation that would result if the risk identified were to materialise
   2) assess the realistic likelihood of the occurrence of the risk identified
   3) determine the levels of risks

e) evaluates the information security risks
   1) compare the results of risk analysis with the risk criteria established, and
   2) prioritise the analysed risks for risk treatment

The Company's risk appetite, criteria for assessing risk and the detailed process on risk assessment and risk treatment are described in *ISMS-PR-01 Information Security Risk Assessment and Risk Treatment Process.*

6.1.2 Information Security Risk Treatment

The organisation defines and applies the information security risk treatment as per *ISMS-PR-01 Information Security Risk Assessment and Risk Treatment Process* to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results

b) determine all controls that are necessary to implement the information security risk treatment options(s) chosen

c) compare the controls determined with the controls set out in the ISO/IEC 27001, and verify that no necessary controls have been omitted, in the context of risks to information security

d) formulate an information security treatment plan

e) obtain risk owners; approval of the information security risk treatment plan and acceptance of the residual information security risks

f) produce a Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justifications for exclusions of controls set out in ISO/IEC 27001 Standard. Justification for exclusion can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the legislation and/or regulation including those applicable to personal data

6.2 ISMS Objectives and Plans to Achieve Them

In accordance with the organisation's information security management policy, the objectives and plans for the ISMS are set out in Appendix D which reflects:

- What will be done
- Resources required
- Responsible parties/personnel
- Completion timeline
- Metrics for evaluation

The organisation's objectives and plans as it relates to the ISMS are tracked and updated as per the completion timeline. The objectives and plans' suitability, adequacy and effectiveness will be reviewed at least once a year. This review may be done during the yearly management review.

6.3 Planning of Changes

When the organisation determines the need for changes to the ISMS, the changes shall be carried out in a planned manner.

The organisation should also consider in its planning and control the monitoring of planned changes, and impact analysis of unexpected changes, to be able to take actions to mitigate adverse effects if necessary.

7 SUPPORT

7.1 Resources

The proper operations and maintenance of the ISMS requires proper personnel planning and resources. The organisation makes sure that the ISMS is properly resourced to guarantee optimal performance, and budget is allocated for any addition resource requirements.

7.2 Competence

The competence of people given responsibility for the ISMS who work under the organisation's control must meet the terms of the ISO/IEC 27001 Standard, to ensure that their performance does not negatively affect the ISMS. Competence can be demonstrated by experience, training and/or education regarding the assumed tasks. When the competence is not enough, training/mentoring must be identified, delivered and assessed to ensure that the required level of competence is achieved.

Details of competency development will be carried out as per *ISMS-PPL-02 Information Security Awareness, Education and Training.*

7.3 Awareness

Awareness is closely related to competence. People who work under the organisation's control must be made aware of:

- The information security policies and objectives;
- Their role and responsibility with regard to information security;
- The implication of changes in the operation of the organisation;
- The importance of conformity with information security policies and procedures, and their role and responsibility in achieving conformity with its requirements;
- The possible consequences to the organisation (e.g., legal consequence, loss of business and brand or reputation damage), to the staff member (e.g., disciplinary consequence) and to the clients of breaching information security rules and procedures; and
- Their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance.

Awareness programme is detailed in *ISMS-PPL-02 Information Security Awareness, Education and Training* and shall be through the following channels:

- briefing / awareness training for ISMS
- documents availability in internal shared repositories accessible to authorised users
- e-mails
- information security meetings

7.4 Communication

Effective communication and consultation channels with interested parties are crucial for the exchange of critical information.

The organisation shall establish, implement, and maintain communication channels for:

- Internal communication amongst employees within the organisation;
- External communication with customers, suppliers, regulatory bodies, and other interested parties;
- Receiving, documenting, and responding to communication from interested parties; and
- Adapting and integrating a threat advisory system, into planning and operational use, if appropriate.

The below communication programme shows a breakdown of the ways in which the necessary information will be communicated to the relevant interested parties:

Interested Party	Subject of Communication	Method(s)	Frequency
Management / Management Representative	Information security strategy High level risk management Policy setting High level reporting	Management Review	At least once a year
	Relevant matters on information security e.g., incidents, threats, risks, changes in legal and other requirements relevant to ISMS, changes in policies, processes and controls relevant to ISMS, review of compliance with information security policies, rules and standards, ISMS resource needs	Information security meetings	Quarterly
Employees	Reporting of risks / incidents / events / observed in day-to-day operation	Emails Arranged briefings	As and when necessary
	Communication of policies, applicable procedures and/or mechanisms	Arranged briefings	Annual briefing
	Ad-hoc reminders on important information security matters	Emails	As and when necessary

Interested Party	Subject of Communication	Method(s)	Frequency
Suppliers	Policies that apply to them Contractual requirements	Contract / agreement Email correspondence / supplier meetings (ad-hoc)	Prior to engagement and during review of performance
Customers	Protection of customer data / personal data Contractual obligations	Contract / agreement Terms of Use Customer meetings (ad-hoc)	Prior to engagement and throughout the duration of the contract
Regulatory bodies	Requested information	As per their instruction	As and when necessary

7.5 Documented information

7.5.1 General

The ISMS documentation shall be established to meet the requirements of ISO/IEC 27001 Standard. The documented information includes the followings:

a. Manual – describe the organisation's overall ISMS and how its processes interact with one another
b. Procedures and Controls Documents – describe the processes and controls as per ISO/IEC 27001 requirements
c. Records (e.g., filled forms, meeting minutes, reports) – demonstrate conformity and effectiveness of the ISMS

7.5.2 Creating and Updating

Documented information created or updated in the scope of the ISMS must be properly identified and described, also considering its content presentation, and any media used. All documented information must undergo proper review and approval to ensure they are fit for purpose as per *ISMS-PR-02 Control of Documented Information.*

7.5.3 Control of Documented Information

The following control shall apply to all documented information for the ISMS:

- Distribution, access, retrieval and use
- Storage and preservation, including preservation of legibility and personal data protection
- Control of changes (e.g., version control)
- Retention and disposition
- Retrieval and use
- Preservation of legibility
- Prevention of the unintended use of obsolete information
- Adequate protection against compromise, loss, unauthorised disclosure or alteration

Detailed procedure on the controls is as per *ISMS-PR-02 Control of Documented Information.*

8 OPERATION

8.1 Operational Planning and Control

To ensure that risks and opportunities are treated properly, information security objectives are achieved, and information security requirements are met, the organisation shall plan, implement, and control its processes, as well as identify and control any relevant outsourced processes by establishing criteria for the processes and implementing control in accordance with the criteria. Documented information deemed as necessary to provide confidence that the processes have been carried out as planned must be retained.

The organisation shall ensure that the ISMS is effectively managed and maintained through:

- Ensuring the continuing relevance of the scope and roles and responsibilities;
- Promoting and embedding continuity across the organisation and other interested parties, where appropriate;
- Managing resources associated with information security;
- Establishing and monitoring change management within the ISMS;
- Arranging and providing appropriate staff training and awareness;
- Implementing actions as determined in the risk assessment and risk treatment process;
- Maintaining ISMS documentation appropriate to the size and complexity of the organisation and keeping it current by implementing best practices;
- Coordinating the regular review and update of information security, including review or reworking information security risk assessments; and
- Ensuring the maintenance of policies and procedures appropriate to the needs of operational controls.

The organisation shall strive to achieve below indicatives of an effective ISMS:

- An incident management capability is enabled and provides an effective response;
- Risk assessment and risk treatment becomes truly proactive and is repeated on a continual basis as an integral part of the business activities;
- The organisation's understanding of itself and its relationships with other organisations, relevant regulators or government agencies, local authorities and the emergency services is properly developed, documented and understood;
- Requirements of interested parties are understood and able to be delivered;
- Client's data are protected;
- Personal data are protected; and
- The organisation remains compliant with its legal and regulatory obligations.

8.2 Information Security Risk Assessment

The organisation shall perform risk assessments at planned intervals and documented information of the results must be maintained according to the criteria defined in *ISMS-PR-01 Information Security Risk Assessment and Risk Treatment Process.*

8.3 Information Security Risk Treatment

Risk treatment plans shall be implemented, retaining the resulting information as documented information as per *ISMS-PR-01 Information Security Risk Assessment and Risk Treatment Process.*

9 PERFORMANCE EVALUATION

9.1 Monitoring, Measurement, Analysis and Evaluation

The organisation shall determine the following:

- What needs to be monitored and measured
- Methods of monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results
- When the monitoring and measuring shall be performed
- When the results from monitoring and measurement shall be analysed and evaluated
- Who shall monitor and measures, and who shall analyse and evaluate the results

The organisation will use data from monitoring and measurement to identify patterns and obtain information regarding its performance. These data are used to ensure that the organisation's policies and objectives are achieved as well as to identify corrective actions and areas for improvement.

The procedure for monitoring, measurement, analysis and evaluation is as per *ISMS-ORG-12 Reviews and Compliance Monitoring.* Records of all periodic monitoring and evaluations shall be maintained as documented information.

9.2 Internal Audit

The organisation shall conduct internal audits at least once a year to ensure the ISMS is achieving its objectives, conforms to its planned arrangements and has been properly implemented and maintained, conforms to the requirements of ISO/IEC 27001 Standard, and to identify opportunities for improvement.

The person responsible for the area being audited shall ensure that any necessary corrections and corrective actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

The procedure to direct the planning and conduct of audits is as per *ISMS-PR-03 Internal Audit.*

9.3 Management Review

Top management shall review the ISMS at least once a year to ensure its continuing suitability, adequacy and effectiveness including the effective operation of its continuity procedures and capabilities.

The organisation shall retain documented information as evidence of the results of the management reviews, communicate the results of the management review to relevant interested parties, and take appropriate action relation to those results.

Detailed process to carry out management review including its inputs and outputs can be found in *ISMS-PR-04 Management Review.*

10 IMPROVEMENT

10.1 Continual Improvement

The organisation will strive to continually improve the suitability, adequacy and effectiveness of the ISMS. This will be driven by the policies and objectives, audit results, analysis of monitoring and measuring data, corrective actions and meetings on different areas of information security at planned intervals including the yearly management reviews.

The procedure to capture continual improvements is further described in *ISMS-ORG-12 Reviews and Compliance Monitoring*.

10.2 Nonconformity and Corrective Action

Nonconformities to the ISMS will be addressed in line with *ISMS-PR-05 Control of Nonconformity and Corrective Action.* This covers how the organisation shall react to the nonconformities, conduct root cause analysis and determine corrective actions appropriate to the effects of the nonconformities encountered.

Nonconformities and the nature of the nonconformities, subsequent actions taken, results of corrective actions shall be retained as documented information as evidence of conformity.

11 APPENDICES

APPENDIX A Table of ISO/IEC 27001 Requirements

The ISMS is developed according to ISO/IEC 27001 Standard. Each requirement of the standard is addressed in the relevant sections of the manual, procedures and control documents as indicated in the table below:

ISO/IEC 27001	Reference Documents
4 Context of the Organisation 4.1 Understanding of the Organisation and its Context 4.2 Understanding the Needs and Expectation of Interested Parties 4.3 Determining the Scope 4.4 Information Security Management System	ISMS-M-01 ISMS Manual section 4
5 Leadership 5.1 Leadership and Commitment 5.2 Information Security Policy 5.3 Organisational Roles, Responsibilities and Authorities	ISMS-M-01 ISMS Manual section 5 Appendix B Information Security Management Policy ISMS-ORG-01 Topic-specific Policies for Information Security ISMS-ORG-02 Information Security Roles & Segregation of Duties
6 Planning 6.1 Actions to Address Risks and Opportunities 6.2 Information Security Objectives and Plans to Achieve Them 6.3 Planning of Changes	ISMS-M-01 ISMS Manual section 6 Appendix C Risks and Opportunities Appendix D ISMS Objectives & Plans ISMS-PR-01 Information Security Risk Assessment & Risk Treatment Process
7 Support 7.1 Resources 7.2 Competence 7.3 Awareness 7.4 Communication 7.5 Documented Information	ISMS Manual section 7 ISMS-PPL-02 Information Security Awareness, Education and Training ISMS-PR-02 Control of Documented Information
8 Operation 8.1 Operational Planning and Control 8.2 Information Security Risk Assessment 8.3 Information Security Risk Treatment	ISMS Manual section 8 ISMS-PR-01 Information Security Risk Assessment & Risk Treatment Process Information Security Controls (ISMS-ORG, ISMS-PPL, ISMS-PHY, ISMS-TECH)
9 Performance Evaluation 9.1 Monitoring, Measurement, Analysis and Evaluation 9.2 Internal Audit 9.3 Management Review	ISMS Manual section 9 ISMS-ORG-12 Reviews and Compliance Monitoring ISMS-PR-03 Internal Audit ISMS-PR-04 Management Review
10 Improvement 10.1 Continual Improvement 10.2 Nonconformity (NC) and Corrective Action	ISMS Manual section 10 ISMS-ORG-12 Reviews and Compliance Monitoring ISMS-PR-05 Control of NC and Corrective Action
Annex A Reference Control Objectives and Controls	Information Security Controls (ISMS-ORG, ISMS-PPL, ISMS-PHY, ISMS-TECH)

APPENDIX B Information Security Management Policy

NetGain Systems is committed to providing holistic and highly flexible IT observability and security management solutions designed to fit the unique demands and deliver excellent service to our clients. We recognize that information security is vital to achieve this commitment. With this understanding, we are committed to the preservation of the confidentiality, integrity and availability of information by implementing a robust Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001.

Our ISMS intends to ensure:

- Confidentiality of all information assets through preserving authorized restrictions on information access and disclosure;
- Integrity of all business processes, information assets, and supporting IT assets and processes, through protection from unauthorized modification or destruction; and
- Availability of all business processes, information assets, and supporting IT assets and processes to authorized users when needed, with timely and reliable access to and use of information.

We strive to stay committed to information security through:

- Complying with laws, regulations and contractual obligations which are applicable to us in general and in particular to ISMS;
- Providing information security training for all employees;
- Continually improving the ISMS and our information security performance; and
- Establishing supporting policies and procedures in a wide variety of information security-related areas to support this policy.

This overarching Information Security Policy and its supporting policies shall be reviewed at least once a year and when significant change occurs to ensure continuing suitability, adequacy, effectiveness and alignment with the strategic direction of the Company. This shall be communicated and understood within the Company, and shall be made available to the appropriate audience, both within and external to, the Company. This Policy shall be implemented consistently throughout the Company.

APPENDIX C Risks and Opportunities

The S.W.O.T Analysis below involves an assessment of our strengths, weaknesses, opportunities and threats in consideration of our relevant internal and external issues, as well as the requirements of our interested parties as defined in sections 4.1 and 4.2 of the ISMS Manual.

This S.W.O.T Analysis leads to our evaluation of the need for a plan of action to prevent unintended outcomes and to take advantage of any opportunities to improve our ISMS.

STRENGTHS • A pioneer in the IT observability, monitoring and data analytics business since 2002 • Local presence throughout the Asia Pacific Region, including Australia, China and Singapore to be able to tap on the growing demand to serve a larger audience • Personalized customer approach with a level of customization designed to fit the unique demands of our customers • Offers a holistic platform, integrated solution and unified console for IT observability and security management	**WEAKNESSES** • Information security risks as per the *Risk Assessment* results • Third-party (e.g., suppliers) information security vulnerabilities
OPPORTUNITIES • More business opportunities and enhanced information security, cybersecurity and privacy with the implementation of ISMS • Expansion to SIEM (Security Information and Event Management) and the Cloud	**THREATS** • New and emerging competition • Cyber security threats • Stricter data protection laws and regulations becoming more and more challenging with substantial fines for failure to comply • Economic factors e.g., lack of customer demand, recession • Force majeure events where the Company has no control of such as acts of God, act of war, action by government, pandemics, natural events, and other disruptive events

The action plans to address the above-mentioned opportunities, weaknesses, and threats while capitalizing on our strengths are listed below:

Opportunities	**Action Plans**

More business opportunities and enhanced information security with the implementation of ISMS	Maintain the ISMS and ensure active ISO/IEC 27001 certificate *Responsible: ISMS MR* *Target: Ongoing efforts*
Expansion to SIEM (Security Information and Event Management) and the Cloud	Explore SIEM and the Cloud and integrate them into product / service offering *Responsible: Strategy Planning and Operations* *Target: Ongoing efforts*
Weaknesses & Threats	**Action Plans**
Information security risks as per the *Risk Assessment* results	*Refer to the Risk Assessment and Risk Treatment Plan for the detailed actions, responsibilities and timelines*
Third-party party (e.g., suppliers) information security vulnerabilities	Implement due diligence assessment and regular performance monitoring of suppliers with respect to information security *Responsible: ISMS MR* *Target: Ongoing efforts*
New and emerging competition	New product / service developments and effective marketing and advertising to survive competition *Responsible: Strategy Planning and Operations* *Target: Ongoing efforts*
Cyber security threats	*Refer to the Risk Assessment and Risk Treatment Plan for the detailed actions, responsibilities and timelines*
Stricter data protection laws and regulations across the globe becoming more and more challenging with substantial fines for failure to comply	Identify applicable legal and other requirements in the context of information security and data protection and review compliance *Responsible: MR / DPO* *Target: Ongoing efforts*
Economic factors e.g., lack of customer demand, recession	Innovative product / service developments with evident cost savings to survive downturn in economy *Responsible: Strategy Planning and Operations* *Target: Ongoing efforts*
Force majeure events where the Company has no control of such as acts of God, act of war, action by government, pandemics, natural events, climate change and other disruptive events	Regularly review and test effectiveness of IT service continuity and disaster recovery *Responsible: ISMS MR* *Target: Yearly*

APPENDIX D ISMS Objectives and Plans

Objective	Target	Action Plans	Required Resources	Responsible Party	Monitoring Frequency	Monitoring Source
Compliance 1. Ensure compliance with legal, regulatory and contractual obligations with respect to information security / data protection	**0** noncompliance	Monitor applicable legal and regulatory changes and developments, and contractual obligations; Take required actions to ensure compliance with applicable requirements	Legal, Regulatory and Contractual Requirements Register; Monitoring of legal/regulatory warnings, violations and breach of contract	ISMS Management Representative (MR)	Monthly monitoring of noncompliance	Legal / regulatory warnings / violation from regulatory authorities / breach of contract
Awareness & Training 2. Ensure employees are well informed about the information security practices and are aware of their information security responsibilities	**100%** completion of information security training annually	Arrange information security employee training at least once a year and maintain attendance	Training Materials	ISMS MR	Yearly conduct of information security training	Attendance Record
Incident 3. Reduce information security incidents to less than 3 incidents per year	**< 3** information security incidents per year	Timely reporting of events for assessment and immediate response if events are categorized as incidents	Reporting channel / tool for incidents; Incident management procedure	Incident Response Team (IRT)	Monthly monitoring of incidents	Incident Tracking Tool

Objective	Target	Action Plans	Required Resources	Responsible Party	Monitoring Frequency	Monitoring Source
Data Breach 4. Prevent notifiable data breach - *Significant scale where it involves personal data of 500 or more individuals* - *Significant harm where it involves personal data (or classes of personal data) as listed in the Personal Data Protection (Notification of Data Breach) Regulations*	**0** notifiable data breach per year	Consistent implementation and compliance review with the organisation's data protection governance policy	Data leakage prevention measures; Reporting channel for data breach; Incident management procedure	DPO	Monthly monitoring of data breach	Data Breach Report
Service Level Agreements (SLAs) Compliance 5. 99.8% SaaS SLA	**99.8%** SaaS SLA compliance	Adding / building redundancy; Detection of failures as they occur	Cloud resources with high availability features	Operations	Monthly monitoring of SLA compliance	SLAs Monitoring Record

Note: The responsible functions shall monitor achievement against the target and communicate the same to the ISMS MR. The ISMS MR shall retain the monitoring summary of the achievement of the objectives against the target set to ensure any negative trends will be addressed promptly.