Information Security Policy

KYG Trade, Inc.

Purpose

KYG Trade, Inc.'s Information Security Policy has been developed to: establish a general approach to information security and the minimization of information misuse, compromise or loss; document security processes and measures; uphold ethical standards and meet the company's regulatory, legal, contractual, and other obligations; control business risk; and ensure that the appropriate company image and reputation is presented.

Scope

This policy applies to:

- Information in any form, regardless of the media on which it is stored, as well as, any facility, system, or network used to store, process, and/or transfer information.
- All KYG Trade, Inc. employees, temporary staff, partners, contractors, vendors, suppliers, and any other person (collectively also referred to as “Staff” or “Personnel”) or entity that accesses the company's networks or any other public or private network through company's networks or systems.
- All activity while using or accessing the company's information or information processing, storage, or transmission equipment, while on the company premises (owned, rented, leased, or borrowed) or remotely.
- Information resources that have been entrusted to the company by any entity external to the company (i.e. Customers, Staff, and others).
- Documents, messages, and other communications created on or communicated via the company systems are considered the company's business records and, as such, are subject to review by third parties in relation to audits, litigation, process improvement, and compliance.

Background

This policy is the overarching policy over the rest of the security policies, which make up the company's information security program (ISP). The series of security policies includes:

- Acceptable Use Policy
- Asset Management Policy
- Backup Policy
- Business Continuity/Disaster Recovery Plans
- Code of Conduct
- Data Classification, Retention, and Protection Policies
- Encryption and Password Policies
- Incident Response Plan
- Physical Security Policy
- Responsible Disclosure Policy
- Risk Assessment Policy
- Software Development Life Cycle Policy
- System Access Management Policy
- Vendor Management Policy
- Vulnerability Management Policy

Information Security Objectives

It is the policy of KYG Trade, Inc. that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information. Ultimately, the information security goal of KYG Trade, Inc. is to maintain:

- Confidentiality: data and information are protected from unauthorized access
- Integrity: Data is intact, complete and accurate
- Availability: IT systems are available when needed

KYG Trade, Inc.'s information security objectives, consistent with the company's information security program are:

- To protect information from all internal, external, deliberate, or accidental threats;
- To enable secure information sharing;
- To encourage consistent and professional use of information;
- To ensure clarity about roles and responsibilities associated with protecting information;
- To ensure business continuity and minimize business damage; and,
- To protect the company from legal liability and the inappropriate use of information.

Roles and Responsibilities

The Operations Manager/CISO is responsible for:

1. The design, development, maintenance, dissemination, and enforcement of the items contained in this policy and other ISP policies.
2. Ensuring that the information security management system conforms to the requirements of ISO/IEC 27001:2013.
3. Reporting on the performance of the information security program to top management.

The objectives and measures outlined by the ISP policies shall be maintained and enforced by the roles and responsibilities specified in each policy and related company documents (e.g., *Skills Matrix*).

Policy Review

At minimum on an annual basis, a of senior management and key personnel will discuss, evaluate and document the company's information security policy, ensuring strategic goals and objectives are continually being developed.

At a minimum on an annual basis, all security policies will be reviewed, modified and/or edited to meet necessary security standards. All policies will be signed and approved by authorized personnel.

Accessibility

Policies and/or procedures will be always made accessible to employees for review via the compliance automation SaaS, *Drata*.

Exceptions

Requests for any exceptions to any policies included within the ISP must be approved by KYG Trade, Inc.'s Executive Management after proper review. Any approved exceptions will be reviewed annually.

Policy

Personnel Security

All personnel will be required to acknowledge in writing their understanding of the Information Security Policy, the Code of Conduct, and other topic-specific policies based on their job function during onboarding and annually thereafter. New hire onboarding will be completed within **90 Days** of hire.

Background checks will be conducted on candidates for employment (employees, temporary personnel, and third parties as deemed necessary) prior to hire using a third-party service provider and in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements. The HR/People team will retain records of the background checks.

Management will evaluate candidates for employment through a formal interview process. The process may include verification of academic and professional qualifications, identity verifications, validation of references, technical interviews, or other steps as deemed applicable based on the job position.

Training

Management will ensure that employees, contractors and third-party users:

- Are properly briefed on their information security roles and responsibilities prior to being granted access to covered information or information systems;
- Are provided with guidelines which state security expectations of their role within the organization;
- Are regularly notified of security changes and updates, as well as reminded of security responsibilities to be undertaken, via annual security awareness training and annual policy acknowledgements;
- Are motivated and comply with the security policies of the organization;
- Achieve a level of awareness on security relevant to their roles and responsibilities within the organization;
- Conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working.

All new hires are required to complete information security awareness training as part of their new employee onboarding process and annually thereafter. Ongoing training will include security and privacy requirements as well as training in the correct use of information assets and facilities. Records to evidence completion of training for all personnel will be retained. The periodic security awareness training will be supplemented with multiple methods of communicating awareness and educating personnel as deemed necessary by management, such as newsletters, web-based training, in-person training, periodic phishing simulations, etc.

The organization will properly communicate to its workforce and, if appropriate, contractors:

- Security updates, changes, and incidents, as needed, via email or appropriate Slack channels.
- Reminders for security responsibilities as part of the annual security awareness training.

In addition, consistent with assigned roles and responsibilities, incident response and contingency training to personnel will be provided:

- Within 90 days of assuming an incident response role or responsibility;
- As required by information system or policy changes; and/or
- Annually.

KYG Trade, Inc. will provide periodic security awareness training to personnel that will cover how to identify and report insider threats. All employees at KYG Trade, Inc. are responsible for reporting potential insider threats promptly through the proper organizational channels.

Cloud Service Customers

KYG Trade, Inc. will develop specific training programs for those involved in the use and management of cloud services, including cloud service business managers, administrators, integrators, and users. The training will address:

- Standards and procedures for the use of cloud services.
- Information security risks related to cloud services and the strategies to manage them.
- The risks associated with system and network environments when using cloud services.
- The legal and regulatory considerations applicable to cloud services

This training will be extended to management and supervisory managers, including those of business units, to ensure the effective coordination of information security activities.

Cloud Service Providers

KYG Trade, Inc. employees are expected to conduct similar awareness, education, and training programs as its cloud service customers.

- KYG Trade, Inc. will instruct contractors to do the same, ensuring the appropriate handling of customer data and data derived from cloud services.
- This data may contain information confidential to a customer or be subject to specific limitations, including regulatory restrictions, on access and use by KYG Trade, Inc..

Intellectual Property Rights

KYG Trade, Inc. takes handling and safeguarding of intellectual property very seriously. Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licenses.

To ensure this the following procedures will be maintained:

- Software will only be acquired through known and reputable sources, to ensure that copyright is not violated.
- An asset inventory will identify all assets with requirements to protect intellectual property rights.
- Proof and evidence of ownership of licenses, master disks, manuals, etc. will be maintained.
- Review of the asset inventory will also make sure that only software and licensed products are installed.
- Will ensure compliance with terms and conditions for software and information obtained from public networks

Cloud Service Customers

When using cloud services, additional procedures will be in place to identify any licensing requirements specific to cloud deployment. This is crucial as installing commercially licensed software in a cloud service may inadvertently breach the terms of the software license. This procedure will give particular attention to scenarios where the cloud service features are elastic and scalable, which may result in the software being used on more systems or processor cores than is permitted by the license terms.

Cloud Service Providers

KYG Trade, Inc. will have an established process for responding to intellectual property rights complaints, ensuring the protection of proprietary assets.

Information Security Requirements Analysis & Specifications

KYG Trade, Inc. will identify its information security requirements through utilizing different methods, ensure the results of the identification are documented and reviewed by all stakeholders, and will integrate the requirements and associated processes in early stages of projects.

Methods

- Policies and regulations
- Threat modeling
- Incident reviews
- Use of vulnerability thresholds

Factors

- Level of confidence required towards the claimed identity of users, in order to derive user authentication requirements.
- Access provisioning and authorization processes, for business and privileged or technical users.
- Informing users and operators of their duties and responsibilities.
- Protection needs of assets, especially in terms of availability, confidentiality, integrity.
- Business processes (e.g., transaction logging and monitoring, non-repudiation requirements).
- Other security controls (e.g. interfaces to logging and monitoring or data leakage detection systems).

Employment Terms and Conditions

The following terms and conditions of employment at KYG Trade, Inc. are the contractual obligations for employees or contractors for the safeguarding of information. They include, but are not limited to:

- Signing a confidentiality or non-disclosure agreement (NDA) prior to access to confidential information and processing facilities.
- Legal responsibilities and rights, particularly concerning intellectual property.
- Responsibilities for the classification of information and management of organizational assets associated with information, information processing facilities and information services handled by an employee or contractor.
- Responsibilities for handling of information received from third parties.
- Reviewing and agreeing with the security policies of the company.
- Duration of responsibilities beyond end of employment.
- Actions to be taken for non-compliance with the terms and conditions, and the company's security policies.

Disciplinary Process

KYG Trade, Inc.'s discipline policy and procedures are designed to provide a structured corrective action process to improve and prevent a recurrence of undesirable employee behavior and performance issues. It has been designed to be consistent with KYG Trade, Inc. cultural values, Human Resources (HR) best practices, and employment laws.

KYG Trade, Inc. reserves the right to combine or skip steps depending on the facts of each situation and the nature of the offense. The level of disciplinary intervention may also vary. Some of the factors that will be considered are whether the offense is repeated despite coaching, counseling, or training, the employee's work record, and the impact the conduct and performance issues have on the organization.

Step 1: Verbal Warning and Counseling

This initial step creates an opportunity for the immediate supervisor to schedule a meeting with an employee to bring attention to an existing performance, conduct or attendance issue. The supervisor should discuss with the employee the nature of the problem or the violation of company policies and procedures. The supervisor is expected to clearly describe expectations and the steps the employee must take to improve performance or resolve the problem.

Step 2: Formal Written Warning

If the employee does not promptly correct any performance, conduct or attendance issues that were identified in Step 1, a written warning will become formal documentation of the performance, conduct, or attendance issues and consequences. The employee will sign a copy of the document to acknowledge receipt and understanding of the formal warning. During Step 2, the immediate supervisor and HR representative will meet with the employee to review any additional incidents or information about the performance, conduct or attendance issues as well as any prior relevant corrective action plans. Management will outline the consequences for the employee of his or her continued failure to meet performance or conduct expectations.

A formal performance improvement plan (PIP) requiring the employee's immediate and sustained corrective action will be issued after a Step 2 meeting. A warning outlining that the employee may be subject to additional discipline up to and including termination if immediate and sustained corrective action is not taken may also be included in the written warning.

Step 3: Suspension and Final Written Warning

There may be performance, conduct, or safety incidents so problematic and harmful that the most effective action may be the temporary removal of the employee from the workplace. When immediate action is necessary to ensure the safety of the employee or others, the immediate supervisor may suspend the employee pending the results of an investigation. Suspensions that are recommended as part of the normal progression of this progressive discipline policy and procedure are subject to approval from a next-level manager and HR.

Step 4: Recommendation for Termination of Employment

The last step in the progressive discipline procedure is a recommendation to terminate employment. Generally, KYG Trade, Inc. will try to exercise the progressive nature of this policy by first providing warnings, a final written warning or suspension from the workplace before proceeding to a recommendation to terminate employment. However, KYG Trade, Inc. reserves the right to combine and skip steps depending on the circumstances of each situation and the nature of the offense. Furthermore, employees may be terminated without prior notice or disciplinary action.

Management's recommendation to terminate employment must be approved by HR and the supervisor's immediate manager. Final approval may be required from the CEO.

Performance and Conduct Issues Not Subject to Progressive Discipline

Behavior that is illegal is not subject to progressive discipline, and such behavior may be reported to local law enforcement authorities. Theft, substance abuse, intoxication, fighting and other acts of violence at work are grounds for immediate termination.

Enforcement

KYG Trade, Inc. Management, under the explicit authority granted by the company CEO, retains the authority and responsibility to monitor and enforce compliance with this Policy and other policies, standards, procedures, and guidelines. Monitoring activities may be conducted on an on-going basis or on a random basis whenever deemed necessary by Management and may require investigating the use of the Company's information resources. The company reserves the right to review any and all communications and activities without notice.

KYG Trade, Inc. will take appropriate precautions to ensure that monitoring activities are limited to the extent necessary to determine whether the communications or activities are in violation of Company policies, standards, procedures, and guidelines or in accordance with normal business processing performance or quality activities.

Violation of the controls established in this Policy is prohibited and will be appropriately addressed. Disciplinary actions for violations may include verbal and/or written warnings, suspension, termination, and/or other legal remedies and will be consistent with our published HR standards and practices.

Relevant Authorities

World Trade Organization (WTO)
The WTO is the only global organization that deals with trade rules between nations. The WTO's goals include helping businesses, providing a forum for trade negotiations, and settling trade disputes. The WTO is run by its member governments, and all major decisions are made by the membership.

U.S. International Trade Administration
The U.S. International Trade Administration's Office of Technology Evaluation (OTE) analyzes U.S. export data, BIS license application data, and global trade information. The OTE's data portal provides data sets and excerpts from statistical reports for the public to analyze.

U.S. Courts
The U.S. Court of International Trade, U.S. Court of Appeals for the Federal Circuit, and U.S. Supreme Court are relevant authorities for trade.

International Courts
Any local court system that maintains jurisdiction within the country of origin that are relevant authorities for trade.

International trade attorneys

International trade attorneys can represent clients before the ITC, the Department of Commerce, or U.S. Customs and Border Protection. They can also help clients with customs classification, valuation, and rules of origin matters.

Other

Other relevant trade data sources include: Census Bureau U.S. Trade in Goods, Bureau of Economic Analysis U.S. Trade in Services, and UN Comtrade Database

Cloud Computing *Cloud Service Customers*

KYG Trade, Inc. will take the following into account for information security in cloud computing:

- Information stored in its cloud computing environment may be accessed and managed by cloud service providers.
- Assets, such as application programs, could be maintained within the cloud computing environment.
- Processes may run on multi-tenant, virtualized cloud service platforms.
- Specific context of cloud service users and the circumstances surrounding the usage of the cloud service.
- Administrators who have privileged access to the cloud service.
- Geographical locations of the cloud service provider's organization and where customer data might be stored, even temporarily.

Cloud Service Providers

KYG Trade, Inc. will address the provision and use of its cloud services, taking the following into account:

- Baseline information security requirements during the design and implementation of cloud services.
- Mitigation of risks associated with authorized insiders.
- Multi-tenancy and cloud service customer isolation, including robust virtualization measures.
- Access controls for staff accessing its cloud service customer assets, including strong authentication mechanisms.
- Effective communication channels with its cloud service customers during change management processes.
- Deployment of robust virtualization security measures.
- Access control for the protection of cloud service customer data.
- Lifecycle management of cloud service customer accounts.
- Communication of security breaches to cloud service customers and providing guidelines and support for investigations and forensics to ensure effective incident response and remediation.

Revision History

Version	Date	Editor	Approver	Description of Changes	DOC ID
1.0	01-March-2025	**Delsean Littlejohn**	**Aslam Latheef**	**First Release**	**IS-001**