TABLE OF CONTENTS

STATEMENT OF COMPLIANCE ................................................................. 3

SECTION 1: REGULATORY COMPLIANCE AND VIOLATIONS .......................... 3

SECTION 2: KEY FORWARDER RESPONSIBILITIES ....................................... 3
  § 2.1 Automated Export System Reporting .................................................. 3
  § 2.2 Communication ................................................................................. 4
  § 2.3 Documentation .................................................................................... 4
  § 2.4 Reporting ............................................................................................ 4
  § 2.5 Performance and Auditing ................................................................. 4

SECTION 3: RECORDKEEPING AND DESTRUCTION POLICIES ...................... 4

SECTION 4: TRAINING AND EDUCATION .................................................. 4

SECTION 5: PENALTIES .................................................................................. 5

SECTION 6: AUTOMATED EXPORT SYSTEM .............................................. 5
  § 6.1 Power of Attorney .............................................................................. 5
  § 6.2 Electronic Export Information Filing .................................................. 6
  § 6.3 AES EEI Filing Training ................................................................. 6

SECTION 7: TRANSPORTATION SECURITY ADMINISTRATION ..................... 7

SECTION 8: CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM .......... 8
  § 8.1 Personnel Security ............................................................................. 8
  § 8.2 Physical Access Controls ................................................................... 8
  § 8.3 Physical Security ................................................................................ 9
  § 8.4 Information Technology Security ..................................................... 9
  § 8.5 Security Procedures .......................................................................... 10
  § 8.6 Procedural Security ......................................................................... 11
  § 8.7 Security Training and Threat Awareness ....................................... 12

SECTION 9: ANTITRUST ................................................................................. 13

SECTION 10: ANTI-BOYCOTT ........................................................................ 13

SECTION 11: HAZARDOUS MATERIALS ....................................................... 14

SECTION 12: DENIED PERSONS & RESTRICTED PARTY SCREENING ......... 15

SECTION 13: INTERNAL AUDITS ............................................................... 16

CONCLUSION ............................................................................................ 16
STATEMENT OF COMPLIANCE

The mission of our export compliance program is to establish and maintain an organizational culture that enforces ethical conduct and a commitment to compliance with all laws, regulations, and policies.

Every employee is encouraged and expected to report anyone or any activity that may be a potential violation of the law, a regulation, ethical conduct, or any company policy to a corporate manager who will direct or escalate the matter as necessary.

Related Documents
Click here to access the Nissin Corporate Charter of Corporate Behavior

SECTION 1: REGULATORY COMPLIANCE AND VIOLATIONS

Regulatory compliance is a corporate priority and everyone’s responsibility to protect our customers and the company. Proactive awareness, education, and enforcement of laws, regulations, and policies are essential to ensure compliance.

All employees must comply with the Code of Federal Regulations (CFR), which is the official and complete text of the general and permanent rules published by the Federal Government, as applicable to their daily operations.

Failure to comply with these requirements will result in

1) Fines or other penalties
2) Lawsuits
3) Legal costs
4) Bad reputation
5) Loss of existing customers
6) Loss of certification(s)

Related Documents
Click here to access the Regulatory Compliance and Violations Training Module and Test

SECTION 2: KEY FORWARDER RESPONSIBILITIES

§ 2.1 Automated Export System Reporting

Maintain proper written authority in accordance with the Federal Trade Regulations (FTR) §30.3(c)(2), such as a Power of Attorney, with expressed authority to file Electronic Export Information (EEI) in the Automated Export System (AES) on behalf of the U.S. Principal Party in Interest (USPPI) or a general written authority for same.

See §5.2 “Electronic Export Information Filing” for more details on EEI filing policies.
§ 2.2 Communication

1) Contact the customer if the Schedule B/HTS numbers are missing. The proper classification must be obtained prior to filing EEI.

2) Respond to customer inquiries no later than one workday.

3) Advise the customer immediately of any federal agency inquiries and actions concerning their export business.

4) Be proactive to continually improve our service to the customer.

§ 2.3 Documentation

Verify all shipment information and perform a quality check of all documents and data to ensure that they are legible, complete, and accurate.

§ 2.4 Reporting

1) Provide ad hoc reports as required by the customer including, but not limited to:
   (a) Historical/Statistical Transaction Data
   (b) Compliance/Error Data
   (c) Amendments/Cancellation/Correction/Timing Data
   (d) Country of Origin/Destination Data
   (e) Value/Classification Data

§ 2.5 Performance and Auditing

1) The U.S. Census Bureau requires a 95% or greater compliance rate for EEI filing to be maintained.
   (a) All branches will be notified by the Compliance and Business Planning Division if the compliance rate falls below the requisite 95%.

SECTION 3: RECORDKEEPING AND DESTRUCTION POLICIES

These policies are required to maintain the integrity, safeguarding, and confidentiality of all hardcopy and electronic records. Each branch and division must manage their documents and data according to these policies.

Related Documents

Click here to access the Recordkeeping and Destruction Procedures

SECTION 4: TRAINING AND EDUCATION

Training and educational outreach is the foundation of a successful export compliance program. Well-informed employees minimize inadvertent violations.

According to their roles and responsibilities, all employees must complete the training listed on the “Compliance Training Checklist” as required at the following levels:

1) Executives: Vice President level and higher

2) Senior Management: Division Managers, Branch Managers, Directors
3) **Middle Management:** Managers, Assistant Managers, Supervisors, Team Leaders  
4) **Staff:** Administrators, Specialists, Coordinators, Agents, Clerks, Material Handlers

**Related Documents**

Click here to access the Compliance Training Checklist

All managers are responsible to ensure their staffs are properly trained, initial and recurrent, to achieve and maintain consistent results and comply with all applicable laws, regulations, and policies. Refer to each section of this manual for references to training modules and tests.

Experienced staff (mentors) should be encouraged to share lessons learned, tips, and suggestions on completing export roles and responsibilities accurately and timely. Mentors can also provide ongoing support to new employees, accelerating their learning curve to achieve the level of understanding required to ensure compliance and reporting accuracy.

Employees who wish to attend seminars and pursue other educational opportunities must request approval from the proper management authority.

**Related Documents**

Click here to access the Employee Handbook  
Click here to access the Tuition Disbursement Form

**SECTION 5: PENALTIES**

Depending on the severity of a violation, a fine can range from $500 (for a mitigated penalty) up to $50,000 for non-compliance. Criminal prosecution may also lead to imprisonment.

Nissin may be charged with the responsibility for involvement in a violation by:

1) Causing, aiding, or supporting a violation  
2) Acting with knowledge of a violation  
3) Conspiracy or evasion  
4) Misrepresentation or concealment of facts  
5) Failure to comply with reporting or recordkeeping requirements

**SECTION 6: AUTOMATED EXPORT SYSTEM**

§ 6.1 **Power of Attorney**

In accordance with the Federal Trade Regulations (FTR) §30.3(c)(2), a valid Power of Attorney (POA), or statement on customer’s letterhead, must be obtained from the customer prior to acting as an authorized agent for export control, U.S. Census Bureau reporting, and U.S. Customs and Border Protection (CBP) purposes.

The POA contains an expressed authority to allow Nissin to prepare and transmit any Electronic Export Information (EEI) or other data required to be filed to the Census Bureau, CBP, the Bureau of Industry and Security, or any other U.S. Government agency.

In addition, Nissin may perform any other act required by law or regulation in connection with
the exportation or transportation of goods shipped or consigned by the U.S. Principal Party in Interest (USPPI) or the Foreign Principal Party in Interest (FPPI) including, but not limited to, conducting security inspections and screening of cargo.

§ 6.2 Electronic Export Information Filing

EEI is the data filed to the AES as the shipper’s formal declaration. It includes all the shipment data required by the government for statistical and security purposes.

EEI must be filed for shipments:

1) From the U.S., Puerto Rico, or the U.S. Virgin Islands to foreign destinations
2) Between the U.S. and Puerto Rico
3) From the U.S. or Puerto Rico to the U.S. Virgin Islands

If the merchandise under the same Schedule B commodity number or Harmonized Tariff Schedule (HTS) valued at US$2,501.00 or more and is sent from the same exporter to the same recipient on the same day. **This value includes U.S. inland freight, insurance, and any other costs up to the final port of export in the U.S. These costs must be prorated by Schedule B/HTS line.**

EEI is not required for shipments:
1) From the U.S. to Canada
2) From the U.S. to the U.S. territories of Guam, Northern Mariana Islands, Midway Island, Wake Island, and American Samoa
3) From the U.S. Virgin Islands to the U.S.
4) From the U.S. Virgin Islands to Puerto Rico

However, if any of the following applies, an EEI must be filed for shipments regardless of value or origin:
1) Has an export license or export permit
2) Is being sent to restricted countries (Refer to Section 11)
3) Is household goods
4) Contains rough diamonds (HTS 7102.10, .21, & .31)

§ 6.3 AES EEI Filing Training

All staff must be trained and made aware of the following EEI filing policies throughout the entire process of receiving & verifying documents, entering data into the AES, responding to error responses and notating loading documents with accurate proof-of-filing citations:

1) **Related Party** status to be reported must be properly determined if USPPI and consignee are related parties or not.
2) **USPPI Name** to be reported must be the person or legal entity in the United States that receives the primary benefit, monetary or otherwise, from the export transaction.
3) **USPPI Address** to be reported must be the location that the goods actually left to begin the journey to the port of export per 15 CFR Part 30 §30.6(a)(1)(ii).
4) Timely filing of EEI in accordance with FTR §30.4(b) must be no later than:
   (a) Vessel: 24 hours prior to loading cargo on the vessel at the U.S. port where
       the cargo is laden
   (b) Truck: 1 hour prior to the arrival of the truck at the U.S. border to go foreign
   (c) Air: 2 hours prior to the scheduled departure time of the aircraft
   (d) Rail: 2 hours prior to the time the train arrives at the U.S. border to go foreign

5) Update and maintain the customers’ approved Schedule B and HTS classifications.

6) Correct “Fatal Errors” and obtain internal transaction number (ITN) prior to
   exportation in accordance with 15 CFR 30.9.

7) Make corrections, cancellations, or amendments to EEI as soon as they are known
   (whether before or after exportation in accordance with FTR §30.9).

8) Maintain pertinent export documents on a per shipment basis for at least five years in
   accordance with FTR §30.10 that include, but are not limited to, the following:
   (a) Commercial Invoice
   (b) Bill of Ladings
   (c) Licenses (if applicable)
   (d) EEI Data Elements
   (e) Electronic Certification Notice

9) Provide export documentation to the customer in accordance with FTR 30.3(c).

Related Documents
Click here to access the AES Training Module and Test

SECTION 7: TRANSPORTATION SECURITY ADMINISTRATION

Nissin has been compliant with the regulations of the Transportation Security Administration (TSA) since 2001 and is a certified Indirect Air Carrier (IAC). Accordingly, we must follow the security parameters of our Indirect Air Carrier Standard Security Program Change 5A (IACSSP).

The purpose of the IACSSP is to provide for the security of persons and property traveling on air transportation against acts of criminal violence and air piracy and against the introduction of any unauthorized person and any unauthorized explosives, incendiary, and other destructive substance or item into cargo onboard a passenger aircraft.

All direct and temporary employees, as well as authorized representatives (A/Rs), who require unescorted access to the warehouse and air cargo must obtain a Security Threat Assessment (STA) approval from TSA. All employees and A/Rs who handle air cargo must also complete the necessary training modules as dictated by TSA.

Related Documents
Click here to access the IAC Certificate
Click here to access the IACSSP Manual Change 5A
SECTION 8: CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM

Nissin has been a certified and validated member of the Customs-Trade Partnership Against Terrorism (C-TPAT) program since 2003. C-TPAT is a voluntary security program enforced by CBP to develop, enhance, and maintain effective security processes throughout the global supply chain to provide the highest level of security to protect the U.S.

C-TPAT is designed to prevent the illegal transportation of weapons of mass destruction, drugs, or other contraband into the U.S. The goal of this policy is to prevent terrorist activity, minimize theft, delays or impounding of product, and inspections & audits.

Related Documents
Click here to access the C-TPAT Certificate

§ 8.1 Personnel Security

All applicants must undergo a background check by the Administration Division. Any applicant who provides misleading or deceptive information to Nissin on an employment form or résumé, or in a selection interview, is immediately eliminated from further consideration for employment.

Nissin may also occasionally find it necessary to investigate current employees, where behavior or other relevant circumstances raise questions concerning safety jeopardy, supply chain security, or work performance.

At times, a background investigation may be appropriate for a promotion, transfer, or change in job responsibilities. Employee investigations may, where appropriate, include credit reports and investigations of criminal records, if any.

Any employee separating from Nissin must undergo an employment termination process to ensure the security of the facility, personnel, and resources.

Related documents:
Click here to access the Background Check Policy
Click here to access the New Hire and Employee Termination Policy
Click here to access the New Hire Checklist for Managers
Click here to access the Separation Procedure
Click here to access the Separation Checklist

§ 8.2 Physical Access Controls

A. Employees and Visitors

1) The Administration Division controls the issuance, removal, and changing of access devices (e.g. keys, key cards, etc).
2) All entry and exit points must be controlled to restrict access to unauthorized persons & vehicles, and should be limited to the smallest possible number.

3) Facility security is the responsibility of all employees.
   (a) Verify the identity of any unknown persons with a photo ID.
   (b) Ensure visitors sign in and out on the “Visitor Log” and wear visitor badges so they are visible at all times.
   (c) Ensure all mail and courier documents are inspected during sorting process.
   (d) Report anything suspicious to management immediately.
      i) Removal of any individual engaged in suspicious activity will be at the discretion of a manager and/or the proper authorities.

**Related documents:**
Click here to access the Access Control Policy
Click here to access the Access & Equipment Security Checklist
Click here to access the Incident Reporting Policy

§ 8.3 Physical Security
All of Nissin's facilities have restricted access which include, but are not limited to, the below security measures to ensure that no vehicle or pedestrian can enter or leave the areas without being properly identified:
   1) Controlled access points
   2) Secured perimeter fencing
   3) Electric or guarded gates
   4) Alarmed entryways after hours
   5) Adequate lighting
   6) Security cameras

The degree of physical security varies based on the facility manager's discretion.

**Related documents**
Click here to access the Access & Equipment Security Checklist
Click here to access the Perimeter Security Policy
Click here to access the Security Alarm Systems Policy
Click here to access the Lock & Key Control Policy
Click here to access the Key & Alarm Code Control List Form
Click here to access the Lighting Policy
Click here to access the CCTV Minimum Policy

§ 8.4 Information Technology Security
Data access must be limited to authorized personnel for business use only. Each employee has a unique User ID and password to access company systems and data. Employees are not to disclose their system access information with anyone.
Unauthorized use of information is strictly forbidden and will result in disciplinary action, including termination of employment and criminal prosecution.

**Related documents**
Click here to access the [IT Security Policy](#)

§ 8.5 Security Procedures

A. Business Partner Requirements AND

§7.5(E) Customer Screening Procedures

In order for a company to be a business partner with Nissin they must have:

1) A verifiable business history
2) A positive business reputation
3) Good standing as a business

If any of the above is not satisfactory, Nissin will remove that company from consideration as a business partner, customer, or vendor.

**Related documents:**
Click here to access the [Business Partner Requirement Policy](#)
Click here to access the [Risk Assessment Policy](#)
Click here to access the [C-TPAT Vendor Security Agreement for Trucker](#)
Click here to access the [C-TPAT Vendor Security Agreement for Co-Loader](#)

B. Point of Origin

Nissin ensures that its business partners comply with C-TPAT minimum security requirements by providing the appropriate security policy(ies) within their scope of responsibility and maintaining an active communication channel to provide guidance for any issues and concerns.

Periodic reviews of their security procedures will be conducted to ensure their continued compliance with C-TPAT minimum security requirements, as necessary.

C. Participation and Certification in Foreign Customs Administrations Supply Chain Security Programs

Currently, our parent company Nissin Corporation in Japan has obtained Authorized Economic Operator (AEO) certification in a supply chain security program being administered by foreign Customs Administration.

If or when any other business partners obtain certification in a supply chain security program being administered by foreign Customs Administration, they will be required to notify us of their participation status.
D. Service Provider Screening and Selection Procedures

All service providers are required to complete a C-TPAT Vendor Security Agreement. Any security concerns are addressed with the service provider directly. In addition, the service provider must agree to allow Nissin to conduct a security audit anytime without notice. If a service provider refuses the agreement or audit, they will be subject to termination.

**Related documents:**

Click here to access the C-TPAT Vendor Security Agreement for Trucker
Click here to access the C-TPAT Vendor Security Agreement for Co-Loader

E. Customer Screening Procedures

See §7.5(A) “Business Partner Requirements.”

F. Container Security - Inspection, Seals, and Storage

Our foreign origin counterparts (point of stuffing) and U.S. facilities (destination) have been trained to maintain container security by inspecting container integrity, checking for signs of tampering, verifying product and quantity prior to loading and at destination, and controlling container seals.

**Related documents:**

Click here to access the Shipping & Receiving Policy
Click here to access the C-TPAT Shipping & Receiving Training Module and Test
Click here to access the Security Inspection Form
Click here to access the Seal Number Discrepancy Procedure

§ 8.6 Procedural Security

Self-assessments and internal audits, as well as CBP validations from point of stuffing at origin through arrival at U.S. port, ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.

A. Documentation Processing

1) Verify all shipment information to ensure that documentation used in the movement of cargo is legible, complete, and accurate.

2) Limit document and data access to authorized personnel for business use only. Unauthorized use of information is strictly forbidden and can result in termination of employment and, in certain cases, criminal prosecution.

3) Report any breach detected in our information security to the immediate supervisor for appropriate action.

B. Manifesting Procedures

1) Obtain shipping advices and manifests from origin prior to arrival of a shipment to verify cargo integrity.

2) Notify management immediately for any discrepancies for appropriate action.
C. Shipping and Receiving

1) Implement minimum shipping and receiving standards to ensure shipment accuracy, security, and receipt of product. All Nissin branches are required to comply with this C-TPAT policy, which is enforced by CBP.

2) Notify management of anything suspicious for appropriate action.

Related documents
Click here to access the Shipping & Receiving Policy
Click here to access the Incident Reporting Policy

D. Cargo Discrepancies

1) Record all discrepancies in seal numbers, products, or quantities (whether over or short), and visible damage on the receiving report. Photographs should be taken of any shipment anomaly.

2) Notify appropriate management for anything suspicious.

3) Management must notify appropriate authorities, as necessary.
   (a) For possible theft or illegal activities: Local law enforcement
   (b) For terrorist threat: CBP, FBI, & local law enforcement

4) In the case of any cargo loss, the facility manager must report to the Compliance and Business Planning Division immediately via phone and follow up with an electronically transmitted incident report within 24 hours.

Related documents
Click here to access the Shipping & Receiving Policy
Click here to access the Incident Reporting Policy

§ 8.7 Security Training and Threat Awareness

A threat awareness program is established and maintained by the Compliance and Business Planning Division to recognize and foster awareness.

Through training, all direct and temporary employees are made aware of the established procedures to address a security related situation (threat awareness) and how to report such a situation, including an escalation to the Compliance and Business Planning Division.

Additional specified training is provided to employees in the shipping and receiving areas, as well as those receiving and opening mail. This specified training includes cargo integrity, protecting access control, seal controls, security inspections, threat awareness, and contraband.

Related documents
Click here to access the C-TPAT General Requirements Training Module and Test
Click here to access the C-TPAT Shipping and Receiving Training Module and Test
SECTION 9: ANTITRUST

Antitrust Law, also known as Competition Law, prohibits unfair business practices or unethical behavior that negatively impacts commerce, trade, and/or consumers. It applies to almost all industries and every level of business, including manufacturing, transportation, and distribution.

All staff must be trained and made aware that, in order to enforce fair and ethical business practices, Antitrust Law prohibits the following activities:

1) Discussion of prices, customers, discounts, costs, surcharges, or terms of sale with Nissin’s competitors
2) Decisions on prices based on competitors or others outside of Nissin
3) Collaborations with competitors
4) Failure to document the source of any sensitive information that an employee may obtain about a competitor to avoid later speculation that the information was improperly obtained
5) Discussion or meeting activities (formal or informal) that appear to violate the antitrust laws

Related Documents
Click here to access the Antitrust Training Module and Test

SECTION 10: ANTI-BOYCOTT

Anti-boycott laws require U.S. firms to refuse participation in foreign boycotts that the U.S. does not approve. These laws prevent U.S. firms from being used to implement foreign policies of other nations that are against U.S. policy.

All staff must be trained and made aware that anti-boycott laws prohibit the following activities:

1) Agreement to refuse or actual refusal to engage in business with Israel
2) Agreement to refuse or actual refusal to engage in business with any other entities not blacklisted by the U.S.
3) Agreement to discriminate or actual discrimination against other persons based on race, sex, religion, national origin, or nationality
4) Providing information about business relationships with or in Israel
5) Providing information about business relationships with or about blacklisted companies not recognized by the U.S.
6) Providing information about the race, sex, religion, national origin, or nationality of another person

Related Documents
Click here to access the Anti-Boycott Training Module and Test
SECTION 11: HAZARDOUS MATERIALS

Hazardous Materials (HAZMAT) are substances, materials, or chemicals that can be capable of posing an unreasonable risk to health, safety, and property.

The purpose of HAZMAT compliance is to protect people and the environment from the risks of HAZMAT transportation. The Department of Transportation (DOT) has established a national policy to set and enforce standards, educate, and conduct research to prevent incidents.

In certain cases, a Competent Authority Approval (CA) may be required for a dangerous good because it is extremely unstable or sensitive to transport.

The CA:

1) is issued and enforced by a U.S. government agency.
2) includes special information and instructions required for handling and shipping.
3) number must be put on the DG Certificate under the “Authorizations” column.
4) copy must be included with the shipping documents for all modes.

Related Documents

Click here to access the DG Certificate and CA Training Module and Test

All direct and temporary employees, as well as authorized representatives (A/Rs), who handle or process HAZMAT must complete the necessary training depending on their responsibilities.

Unlike the majority of Nissin’s compliance training, the five types of HAZMAT training, as listed below, are primarily outsourced to third party organizations.

1) General Awareness/Familiarization Training: Provides a familiarity with the general requirements of HMR and enables the HAZMAT employee to recognize and identify hazardous materials. All HAZMAT employees must complete this training.

2) Function-Specific Training: Provides a detailed understanding of HMR applicable to the function(s) performed by the HAZMAT employee. HAZMAT employees must be trained on the specific functions they are required to perform in their duties.

3) Safety Training: Provides an overview of the hazards presented by HAZMAT, safe handling, emergency response information, and how to avoid accidents. All HAZMAT employees must complete this training.

4) Security Awareness Training: Provides a general understanding of the security risks associated with HAZMAT transportation and the methods designed to enhance transportation security. The training should include methods to recognize and respond to possible security threats. All HAZMAT employees must complete this training.

5) In-Depth Security Training: Provides a detailed understanding of a company’s security plan including company security objectives, specific security procedures, employee responsibilities, actions to take in the event of a security breach and the organizational security structure. HAZMAT employees who handle or perform regulated functions related to the transportation of the materials covered by the
security plan or who are responsible for implementing the security plan must receive this training.

SECTION 12: DENIED PERSONS & RESTRICTED PARTY SCREENING

Denied Persons and Restricted Parties are companies, entities, or individuals that have had their export privileges suspended, revoked, or otherwise controlled by U.S. government agencies.

Below are links to the export screening lists of the Departments of Commerce, State, and the Treasury as an aide to conduct electronic screens of potential parties of concern.

In the event that a company, entity, or individual on the list appears to match a party potentially involved in your export transaction, additional due diligence must be conducted before proceeding. There may be a strict export prohibition, requirement for seeking a license application, evaluation of the end-use or user to ensure it does not result in an activity prohibited by any U.S. export regulations, or other restriction. If a corporation is found guilty of terrorist activity they may be subject to fines and penalties up to $10 million and/or imprisonment.

Prior to taking any further actions, you must consult the requirements of the agency’s webpage upon whose list the company, entity, or individual appears.

1) Department of Commerce – Bureau of Industry and Security (BIS)
   (a) Denied Persons List – Entities and individuals on this list have been denied export privileges. Any dealings with a party on this list that would violate the terms of its denial order are prohibited.
   (b) Unverified List – End-users who BIS has been unable to verify in prior transactions. The presence of a party on this list in a transaction is a “Red Flag” that should be resolved before proceeding with the transaction.
   (c) Entity List – Parties whose presence in a transaction can trigger a license requirement supplemental to those elsewhere in the Export Administration Regulations (EAR). The list specifies the license requirements and policy that apply to each listed party.

2) Department of State – Bureau of International Security and Non-Proliferation
   (a) Nonproliferation Sanctions – Parties that have been sanctioned under various statutes. Although the linked webpage is updated as appropriate, refer to the Federal Register, which is the only official and complete listing of nonproliferation sanctions determinations.

3) Department of State – Directorate of Defense Trade Controls
   (a) AECA Debarred List – Entities and individuals prohibited from participating directly or indirectly in the export of defense articles, including technical data and defense services. Pursuant to the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), the AECA Debarred List includes persons convicted in court of violating or conspiring to violate the AECA and subject to “statutory debarment” or persons established to have violated the AECA in an administrative proceeding and subject to “administrative debarment.”
4) Department of the Treasury – Office of Foreign Assets Control
   (a) Specially Designated Nationals List – Parties who may be prohibited from export transactions based on OFAC’s regulations. The EAR require a license for exports or re-exports to any party in any entry on this list that contains any of the suffixes “SDGT,” “SDT,” “FTO,” “IRAQ2,” or “NPWMD.”

These lists are updated by their respective government agencies. Nissin must screen any potential customers to ensure we do not engage in a transaction with a barred company, entity, or individual. Records of these screenings must be kept according to the Recordkeeping Policy.

SECTION 13: INTERNAL AUDITS

Nissin monitors compliance, develops continuous improvements, and adds value to our customer service through the results of our internal audits.

Internal audits bring a systematic, disciplined approach to evaluate and improve the effectiveness of corporate governance and operations management processes.

The primary components of internal audits are:

1) Audit Interviews and Document/Data Review
2) Operational and Compliance Assessment
3) Determination of Corrective and Preventive Actions
4) Implementation of Corrective and Preventive Actions

The assessments focus on regulatory compliance, customer satisfaction, operational efficiency, and opportunities for improvement.

Internal audit results and recommendations are reported to the company President and Board of Directors without prejudice or reservation.

Related Documents
Click here to access the Internal Audit Procedures
Click here to access the Corporate Internal Audit Assessment Form
Click here to access the Operational Internal Audit Assessment Form
Click here to access the Corrective Action Procedures

CONCLUSION

Compliance with government regulations and corporate policies is critical to protect Nissin’s business and employees now and in the future.