Personal Data Processing Addendum

Introduction

A. This Personal Data Processing Addendum, together with its Annexes, (collectively, the "**DPA**") is entered into between Customer, also on behalf of its affiliates (where this is established in the Service Agreement) ("**Client**") and Aramex, also on behalf of its affiliates (where this is established in the Service Agreement) ("**Aramex**") to reflect the Parties' agreement related to the Processing of the Client Personal Data, in accordance with the requirements of the Applicable Data Protection Laws.

B. Aramex has agreed to provide the services to Client ("**Service**") under the terms of the agreement between the Parties ("**Service Agreement**"), to which this DPA is annexed. In order to provide this Service, Aramex may need to Process Personal Data on behalf of Client.

C. The purpose(s) purposes of the Processing of Client Personal Data related to the Service is/are more fully described in Annex 1 of this DPA.

D. Client acknowledges that its use of the Service may be subject to the Applicable Data Protection Laws of varied jurisdictions, which may impose certain obligations related to the Processing of Personal Data upon the Client and/or Aramex.

E. The Parties entered into this DPA to ensure compliance with the Applicable Data Protection Laws and establish safeguards and procedures for the lawful Processing of Personal Data. Client confirms that the provisions laid down in this DPA reflect the obligations that the Applicable Data Protection Laws require Aramex to comply with, regarding the Processing of Client Personal Data in the context of the provision of the Service. Accordingly, Aramex undertakes to comply with the provisions set forth in this DPA.

1. DEFINITIONS

Unless otherwise defined in this DPA, all terms in capital letters used in this DPA will have the meaning given to them in the Service Agreement. In the event of any conflict or inconsistency in terms of data protection safeguards between this DPA and the Service Agreement, this DPA will prevail.

Adequacy Decision: a legally-binding decision issued by the European Commission, allowing the transfer of Personal Data from the EEA to a third country which has been considered adequate in terms of data protection safeguards;

Applicable Data Protection Laws: in EU Member States, the Regulation and complementary national data protection laws, including any guidance and/or codes of practice issued by the relevant Supervisory Authorities within the EU; in non-EU countries, any applicable data protection laws regarding the safeguarding and lawful processing of Personal Data;

Client Personal Data: Personal Data, relating to Data Subjects, Processed in connection with the Service provided by the Data Processor to the Client;

Data Controller: in general, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. For the purposes of this DPA, the Data Controller is the Client;

Data Exporter has the meaning set forth in the Standard Contractual Clauses.

Data Importer has the meaning set forth in the Standard Contractual Clauses.

Data Processor: in general, a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller. For the purposes of this DPA, the Data Processor is Aramex;

Data Subject has the meaning set forth in the Regulation;

Data Subjects' Rights: the rights which Data Subjects are entitled to under the Applicable Data Protection Laws. To the extent that the Regulation is applicable, **Data Subjects' Rights** include, e.g., the right to request access to, rectification or erasure of Personal Data, to request the restriction of Processing concerning the Data Subject or to object to Processing, as well as the right to data portability, from the Data Controller;

DPA: this Global Data Processing Agreement, together with Annexes 1 and 2;

EEA: the European Economic Area;

EU: the European Union;

List of Sub-processors: means the list of Sub-processors which may be made available to the Data Controller upon request, subject to the terms defined in Clause 5.

Non-EEA Entity: any entity, acting as Data Processor (or Sub-processor), located in a country outside of the EEA or which has not received an Adequacy Decision, which Processes Client Personal Data in the context of the provision of the Service;

Personal Data: any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. For the avoidance of doubt, **Personal Data** has the meaning as set forth in the Regulation and the Applicable Data Protection Laws;

Process or **Processing:** any operation, or set of operations, which is performed on Personal Data, or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

Special Categories of Personal Data: Personal Data that reveals: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of natural persons, as well as genetic data, biometric data (when Processed for the purpose of uniquely identifying a natural person), data concerning health or data concerning a natural person's sex life or sexual orientation, including data relating to criminal convictions and offences or related security measures;

Standard Contractual Clauses: the standard contractual clauses for the transfer of Personal Data from a EU Data Controller to a Non-EEA Entity acting as Data Processor adopted by the European Commission in its Decision 2010/87/UE on 5 February 2010, including its Appendices 1 and 2 (Annexes 1 and 2 of this DPA);

Sub-processor: an entity engaged by the Data Processor to assist it in (or who undertakes any part of) Processing the Client Personal Data, in fulfilment of the Data Processor's obligations under this DPA, as identified in the List of Sub-processors, which has been approved by the Data Controller under Clause 5 of this DPA.

Supervisory Authority: any authority which has powers to monitor and enforce the application of the Applicable Data Protection Laws regarding the Processing of Client Personal Data in the context of the provision of the Service.

2. DATA PROTECTION ROLES

The Parties agree that:

a) The Client is Data Controller regarding Client Personal Data Processed by Aramex in the context of the provision of the Service;

b) Aramex is a Data Processor regarding the Client Personal Data Processed in the context of the provision of the Service; and

c) This DPA governs the relationship between the Parties in terms of respective duties and obligations concerning the Processing of Client Personal Data by Data Processor in the context of the provision of the Service.

3. OBLIGATIONS OF THE DATA PROCESSOR

3.1. Data Controller determines the purposes for which Client Personal Data is Processed in the context of the provision of the Service.

3.2. Aside from the obligations listed in Annexes 1 and 2 of this DPA, Data Processor further commits to complying with the following obligations:

a) Data Processor will Process Client Personal Data only as necessary to provide the Service and subject to Data Controller's written instructions provided in this DPA. For these purposes, the Service Agreement and this DPA set out Data Controllers' complete instructions to Data Processor in relation to the Processing of Client Personal Data – any Processing required which is outside the scope of these instructions (including the rights and obligations laid down in the MSA) will require prior written agreement between the Parties;

b) Data Processor will notify Data Controller in the event that it considers a specific written instruction received from Data Controller to be in violation of the Applicable Data Protection Laws. In no case will Data Processor be under any obligation to perform a comprehensive legal examination of any written instructions provided by the Client;

c) Aramex, as Data Processor, will notify Data Controller without undue delay of any contact, communication or correspondence it may receive from a Supervisory Authority, related to the Processing of Client Personal Data. Both Parties acknowledge and agree that the responsibility for replying to such contacts, communications or correspondence rests solely on Data Controller, and not on Data Processor;

d) Data Processor has implemented adequate operational, technical and organisational measures under Article 32 of the Regulation (which are described in Annex 2 of this DPA), to protect the Client Personal Data (including Special Categories of Personal Data). The Parties acknowledge and agree that Data Processor is specifically allowed to implement adequate alternative measures or use alternative locations to Process the Client Personal Data, so long as the security level of the measures is maintained and is, in all respects, adequate;

e) In the event that Data Processor discloses Client Personal Data to its personnel which is directly and exclusively involved in the provision of the Service, Data Processor will ensure that such personnel:

i) is committed to confidentiality or is under an appropriate statutory obligation of confidentiality; and

ii) Processes Client Personal Data under the instructions of Data Processor, and in compliance with Data Processor's obligations under this DPA.

4. OBLIGATIONS OF THE DATA CONTROLLER

4.1. Data Controller acknowledges and agrees that, in order for Data Processor to provide the Service, Data Controller must provide the Client Personal Data to Data Processor.

4.2. Data Controller represents and warrants that:

a) It has an appropriate legal basis (e.g., Data Subjects' consent, legitimate interests, authorisation from the relevant Supervisory Authority) to Process and disclose the Client Personal Data to Data Processor, in the context of the provision of the Service; and

b) the provisions laid down in this DPA reflect the obligations that the Applicable Data Protection

Laws require Aramex to comply with, regarding the Processing of Client Personal Data in the context of the provision of the Service.

5. CONSENT TO SUB-PROCESSING

5.1. Data Controller acknowledges, agrees and consents that, for the sole and exclusive purpose of providing the Service and subject always to compliance with the terms of this DPA, Client Personal Data may be Processed by Data Processor or its Sub-processors, as identified in the List of Sub-processors.

5.2. As such, Data Controller hereby provides a general authorisation to Data Processor for the engagement of Sub-processors, provided that Data Processor:

a) provides Data Controller, at Data Controller's request, with the List of Sub-processors, including the identity, location and role performed by Sub-processors engaged to provide the Service;

b) notifies Data Controller of any update to the List of Sub-processors, so that Data Controller may object to the engagement of any specific Sub-processors, under the terms of Clause 5.3;

c) enters into written agreements with each Sub-processor, binding them to the same obligations concerning the Processing of Client Personal Data as Data Processor is bound to under this DPA;

d) exercises appropriate due diligence in selecting Sub-processors and retains liability for Sub-processors' compliance with their obligations under this DPA;

e) informs Data Controller, to a reasonable extent, as to actions and measures Data Processor and its Sub-processors have undertaken to comply, in practice, with the provisions set forth in this DPA, at Data Controller's request.

5.3. Requests to be provided with the List of Sub-processors should be sent by Data Controller to the following address: dpo@aramex.com. Once the List of Sub-processors has been provided to Data Controller, Data Processor will send notifications to Data Controller regarding the addition or replacement of specific Sub-processors included in the List of Sub-processors, for the purposes mentioned in Clause 5.2(b).

5.4. Data Controller may be required to accept appropriate non-disclosure and non-solicitation obligations, without which the List of Sub-processors may be withheld by Data Processor.

6. TRANSFER OF PERSONAL DATA AND INCORPORATION OF STANDARD CONTRACTUAL CLAUSES

6.1. To the extent that the Regulation is applicable and there are no Adequacy Decisions, Data Controller and Data Processor commit to complying with the obligations laid down in the Standard Contractual Clauses, which are hereby accepted by both Parties as incorporated into this DPA. Moreover, Data Controller expressly authorises Data Processor to enter into written agreements containing the Standard Contractual Clauses with Non-EEA Entities (Sub-Processors) on behalf of Data Controller.

6.2. Under the terms set out in Clause 6.1, the Parties acknowledge that Annexes 1 and 2 of this DPA will apply and be deemed as Appendices 1 and 2 of the Standard Contractual Clauses. Data Controller hereby authorises Data Processor to unilaterally amend Appendices 1 and 2 of the Standard Contractual Clauses only to the extent that any amendment imposes stricter obligations on the Non-EEA Entities.

6.3. Nothing in this DPA shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses.

6.4. Data Controller may request an opportunity to review the Standard Contractual Clauses, including Appendices 1 and 2, from Data Processor.

6.5. Data Controller acknowledges that it is Data Controller's responsibility to comply with any additional applicable duties and obligations required in order to make the transfer of Personal Data to Data Processors and Sub-processors lawful, under the Applicable Data Protection Laws.

7. COOPERATION AND ACCOUNTABILITY OBLIGATIONS

7.1. The Parties will cooperate in good faith, in order to ensure compliance with the provisions of this DPA, including, but not limited to, assuring the correct and timely exercise of Data Subjects' Rights, managing incidents in the event of a security/Personal Data Breach so as to mitigate their possible adverse effects, etc.

7.2 The Parties will cooperate in good faith, in order to make available to each other, as well as to Supervisory Authorities, all information necessary to demonstrate compliance with the Applicable Data Protection Laws.

8. DATA SUBJECT RIGHTS

8.1. Taking into account the nature of the Processing, Data Processor will assist Data Controller in the fulfilment of Data Controller's obligation to respond to requests to exercise Data Subjects' Rights, by means of appropriate technical and organisational measures.

8.2. Data Processor will cooperate with and assist Data Controller, to a reasonable extent, and provide such information as may reasonably be required to respond to Data Subjects' Rights requests, or otherwise to enable Data Controller to comply with its duties related to Data Subjects' Rights under the Applicable Data Protection Laws. Data Controller acknowledges and agrees that, in the event that this cooperation and assistance requires a significant amount of resources on the part of Data Processor, this assistance will be chargeable to Data Controller, upon prior notice and with Data Controller's agreement.

9. DATA RETURN AND DELETION

9.1. Data Processor will, at no cost to Data Controller, return or destroy the Client Personal Data at Data Controller's request. Furthermore, upon the expiration or earlier termination of this DPA, Data Processor will, at no cost to Data Controller, return or destroy the Client Personal Data to Data Controller, subject to a written request of Data Controller with reasonable advance notice. This will not apply where mandatory applicable laws (including, but not limited to, the Applicable Data Protection Laws) or binding orders from law enforcement authorities (including, but not limited to, the Supervisory Authority), prevent Data Processor from doing so.

9.2. Without prejudice to Clause 9.1, Data Processor will comply with requests from Data Controller to return the Client Personal Data to the extent that they are feasible, subject to commercially reasonable technical and organisational constraints, commensurate with the volume, categories and amount of Client Personal Data Processed by Data Processor.

9.3. Client Personal Data which is returned following Data Processor's standard internal procedure will be returned at no cost to the Client; if an alternative procedure is followed, at the Client's request, it will be returned at a reasonable cost.

9.4. Without prejudice to Clauses 9.1 and 9.5, if Data Controller chooses to have the Client Personal Data deleted, Data Processor will provide a statement assuring such deletion to Data Controller.

9.5. Data Processor may retain Client Personal Data which is stored in accordance with regular computer back-up operations, in compliance with Data Processor's disaster recovery and business continuity protocols (see Clause 12), provided that Data Processor may not, and must not allow its Sub-processors to, actively or intentionally Process such Client Personal Data for any purpose other than to provide the Service.

10. DATA TRANSMISSIONS

10.1. Personal Data which is transmitted via the Internet by Data Processor in the context of the provision of the Service will be reasonably encrypted. The Parties acknowledge, however, that the security of transmissions over the Internet cannot be guaranteed. Data Processor will not be responsible for ensuring Data Controller's access to the Internet, nor for any interception or interruption of any communications made over the Internet, or for changes to or losses of Personal Data transmitted via the Internet.

10.2. If a Personal Data Breach is suspected, Data Processor may suspend Data Controller's use of the Service via the Internet immediately, pending an investigation, provided that Data Processor notifies Data Controller of this suspension as soon as reasonably possible, takes all reasonable measures to promptly restore use of the Service via the Internet and cooperates with Data Controller in order to continue providing the Service via alternative communication channels.

10.3. Data Controller must take all adequate and reasonable actions necessary to maintain the confidentiality of the usernames and passwords used by employees (or other collaborators) of Data Controller in the context of the provision of the Service. Data Controller will be liable for the consequences of any misuse of the Service by any of its employees (or other collaborators).

11. PERSONAL DATA BREACH

11.1. Data Controller acknowledges and agrees that Data Processor will not be held responsible for any Personal Data Breaches which are not imputable to Data Processor's negligence or wilful misconduct.

11.2. If Data Processor becomes aware of a Personal Data Breach, it will:

a) take appropriate actions to contain and mitigate the Personal Data Breach, including notifying Data Controller as soon as possible, but in no event later than forty-eight (48) hours after Data Processor becomes aware of the Personal Data Breach, in order to enable Data Controller to expeditiously implement its response programme. Notwithstanding the above, Data Processor reserves the right to determine the measures it will take to comply with the Applicable Data Protection Laws or to protect its own rights and interests;

b) cooperate with Data Controller to investigate the nature, categories and approximate number of affected Data Subjects, the categories and approximate number of affected Personal Data records and the likely consequences of the Personal Data Breach, in a manner which is commensurate with its seriousness and its overall impact on Data Controller and the provision of the Service under this DPA;

c) where the Applicable Data Protection Laws require that the Personal Data Breach be notified to relevant Supervisory Authorities and affected Data Subjects, defer and take instructions from Data Controller, to the extent in which Client Personal Data is involved in the Personal Data Breach –Data Controller is exclusively entitled to determine the measures to be taken in order to comply with the Applicable Data Protection Laws or to remediate any risk, including, without limitation:

i. whether notice is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others, as may be required by the Applicable Data Protection Laws, or at Data Controller's discretion; and

ii. the contents of such notice, whether any type of remediation may be offered to affected Data Subjects under the Client's responsibility, and the nature and extent of any such remediation.

12. DISASTER RECOVERY AND BUSINESS CONTINUITY

Data Processor must maintain commercially reasonable disaster recovery and business continuity protocols, and must provide a summary of these protocols to Data Controller upon request. Data Processor agrees to comply with these protocols, and may amend them at any time, provided that its disaster recovery capacity is not lowered by any amendment to lesser than the effective disaster recovery capacity as existing on the date on which this DPA is entered into.

13. MANDATE

13.1. By signing this DPA, including its Annexes 1 and 2, Data Controller explicitly mandates Data Processor to carry out, on its behalf, the activities described in Clauses 5 and 6.

13.2. By signing this DPA, Data Processor explicitly accepts the mandate mentioned in Clause 13.1 above, which will be carried out without economic remuneration in that it is carried out in connection with the Service, and legally signifies that Data Processor has read and understood the instructions assigned.

ANNEX 1 (Appendix 1 to the Standard Contractual Clauses, where applicable)

1. DATA EXPORTER

The data exporter is the Data Controller, as defined in Clause 1 of DPA, or Data Processor, as authorised by Data Controller under Clause 6 of the DPA.

2. DATA IMPORTER

The data importer is the Data Processor, as defined in Clause 1 of the DPA, or the Sub-processor, as authorised by Data Controller under Clauses 5 and 6 of the DPA.

3. DATA SUBJECTS

The personal data transferred concern the following categories of Data Subjects: consignees, shippers, employees

4. CATEGORIES OF PERSONAL DATA

The personal data transferred concern the following categories of data: name, surname, telephone numbers, address, email address

5. SPECIAL CATEGORIES OF DATA (IF APPROPRIATE)

The personal data transferred concern the following special categories of data (please specify): N/A

6. PROCESSING OPERATIONS

The personal data transferred will be subject to the following basic Processing activities (please specify):
Personal Data may be transferred only for the provision of the Service as described in the Service Agreement.

ANNEX 2 (Appendix 2 to the Standard Contractual Clauses, where applicable)
Description of the Technical and Organisational Security Measures

The Data Processor and the Sub-processors undertake to maintain no less than the technical and organisational measures described below.

Information security policies

Management direction for information security
Management should define a set of policies to clarify their direction of, and support for, information security. At the top level, there should be an overall "information security policy" as specified in ISO/IEC 27001 section 5.2.

Organization of information security

Internal organization
The organization should lay out the roles and responsibilities for information security and allocate them to individuals. Where relevant, duties should be segregated across roles and individuals to avoid conflicts of interest and prevent inappropriate activities.

Mobile devices and teleworking
There should be security policies and controls for mobile devices (such as laptops, tablet PCs, wearable ICT devices, smartphones and other USB gadgets) and teleworking (such as telecommuting, working-from home and remote/virtual workplaces).

Human resource security

Prior to employment
Information security responsibilities should be taken into account when recruiting permanent employees, contractors and temporary staff (e.g. through adequate job descriptions, pre-employment screening) and included in contracts (e.g. terms and conditions of employment and other signed agreements defining security roles and responsibilities, compliance obligations etc.).

During employment
Managers should ensure that employees and contractors are made aware of and motivated to comply with their information security obligations. A formal disciplinary process is necessary to handle information security incidents allegedly caused by workers.

Termination and change of employment
Security aspects of a person's departure from the organization, or significant changes of roles within it, should be managed, such as returning corporate information and equipment in their possession, updating their access rights, and reminding them of their ongoing obligations under privacy and intellectual property laws, contractual terms etc. plus ethical expectations.

Asset management

Responsibility for assets
All information assets should be inventoried and owners should be identified to be held accountable for their security. 'Acceptable use' policies should be defined and assets should be returned when people leave the organization.

Information classification
Information should be classified and labelled by its owners according to the security protection needed, and handled appropriately.

Media handling
Information storage media should be managed, controlled, moved and disposed of in such a way that the information content is not compromised.

Access control

Business requirements of access control
The organization's requirements to control access to information assets should be clearly documented in an access control policy and procedures. Network access and connections should be restricted.

User access management
The allocation of access rights to users should be controlled from initial user registration through to removal of access rights when no longer required, including special restrictions for privileged access rights and the management of passwords (now called "secret authentication information") and regular reviews and updates of access rights should take place.

User responsibilities
Users should be made aware of their responsibilities towards maintaining effective access controls e.g. choosing strong passwords and keeping them confidential.

System and application access control
Information access should be restricted in accordance with the access control policy e.g. through secure log-on, password management, control over privileged utilities and restricted access to program source code.

Cryptography

Cryptographic controls
There should be a policy on the use of encryption, plus cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management.

Physical and environmental security

Secure areas
Defined physical perimeters and barriers, with physical entry controls and working procedures, should protect the premises, offices, rooms, delivery/loading areas etc. against unauthorized access. Specialist advice should be sought regarding protection against fires, floods, earthquakes, bombs, etc.

Equipment
"Equipment" (meaning ICT equipment, mostly) plus supporting utilities (such as power and air conditioning) and cabling should be secured and maintained. Equipment

and information should not be taken off-site unless authorised, and must be adequately protected both on and off-site. Information must be destroyed prior to storage media being disposed of or re-used. Unattended equipment must be secured and there should be a clear desk and clear screen policy.

Operations security

Operational procedures and responsibilities
IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Capacity and performance should be managed. Development, test and operational systems should be separated.

Protection from malware
Malware controls are required, including user awareness.

Backup
Appropriate backups should be taken and retained in accordance with a backup policy.

Logging and monitoring
System user and administrator/operator activities, exceptions, faults and information security events should be logged and protected. Clocks should be synchronized.

Control of operational software
Software installation on operational systems should be controlled.

Technical vulnerability management
Technical vulnerabilities should be patched, and there should be rules in place governing software installation by users.

Information systems audit considerations
IT audits should be planned and controlled to minimize adverse effects on production systems, or inappropriate data access.

Communications security

Network security management
Networks and network services should be secured, for example by segregation.

Information transfer
There should be policies, procedures and agreements (e.g. non-disclosure agreements) concerning information transfer to/from third parties, including electronic messaging.

System acquisition, development and maintenance

Security requirements of information systems
Security control requirements should be analysed and specified, including web applications and transactions.

Security in development and support processes
Rules governing secure software/systems development should be defined as policy. Changes to systems (both applications and operating systems) should be controlled. Software packages should ideally not be modified, and secure system engineering principles should be followed. The development environment should be secured, and outsourced development should be controlled. System security should be tested and acceptance criteria defined to include security aspects.

Test data
Test data should be carefully selected/generated and controlled.

Supplier relationships

Information security in supplier relationships
There should be policies, procedures, awareness etc. to protect the organization's information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed within the contracts or agreements.

Supplier service delivery management
Service delivery by external suppliers should be monitored and reviewed/audited against the contracts/agreements. Service changes should be controlled.

Information security incident management

Management of information security incidents and improvements
There should be responsibilities and procedures to manage (report, assess, respond to and learn from) information security events, incidents and weaknesses consistently and effectively and in order to collect forensic evidence.

Information security aspects of business continuity management

Information security continuity
The continuity of information security should be planned, implemented and reviewed as an integral part of the organization's business continuity management systems.

Redundancies
IT facilities should have sufficient redundancy to satisfy availability requirements.

Compliance

Compliance with legal and contractual requirements
The organization must identify and document its obligations to external authorities and other third parties in relation to information security, including intellectual property, [business] records, privacy/personally identifiable information and cryptography.

Information security reviews
The organization's information security arrangements should be independently reviewed (audited) and reported to management. Managers should also routinely review employee and system compliance with security policies, procedures, etc. and initiate corrective actions where necessary.