Executive Office Instruction Ref. EOI.IAIG.2019.01
Privacy and Information Security Governance

Authority:

This Executive Office Instruction (EOI) is promulgated by the Director, Internal Audit and Investigations Group (IAIG) under the Executive Office Directive on Privacy and Information Security (Ref. EOD.ED.2019.02) on the basis of a delegation of authority by the Executive Director.

Purpose

The purpose of this EOI is to provide instructions on the governance and management of personal data privacy and information security across the operational footprint of the organization.

Effective Date:

This EOI shall become effective immediately.

[signature redacted]

Paul Lucas
Director, IAIG

1. Privacy and Information Security Governance Functions

1.1. In order to deliver effective oversight for all activities related to the governance, risk management, and overall control of privacy and information security arrangements within the organization, the Executive Director (ED) has authorized the Chief Information Security Officer (CISO) to develop the organization's privacy governance framework, addressing key areas such as leadership & governance, planning & strategy, program delivery, incident management, and evaluation & reporting. The CISO is also authorized to develop a system by which the organization directs and controls information security, including key areas such as policy development, information security investment, coordination across departments, and risk management.

1.2. The Privacy and Security Incident Response Team (PSIRT) will serve as the first responder to privacy and computer security incidents and perform vital functions in identifying, mitigating, reviewing, documenting, and reporting findings to the ED and the Senior Leadership Team (SLT).

1.3. The CISO will serve in an advisory capacity to the ED and the SLT on privacy and information security strategic matters and the PSIRT will provide services and support to the organization pertaining to the prevention, management, and coordination of privacy and information security-related emergencies. All final decisions on privacy and security matters will be made by the ED and SLT.

1.4. The CISO will engage, collaborate, and coordinate with individuals across the organization to ensure that collective intelligence is at the core of key activities. Key thought partners will include representatives from safety & security, ICT, internal audit, legal, human resources, enterprise risk management (ERM), etc. Inputs from these functions will ensure that the ED and SLT receive the expert advice required to implement privacy and information security controls and policy requirements that are strong, appropriate, and in alignment with the organization's mission.

1.5. The PSIRT will include the CISO and the individuals responsible for storage and other data repositories, computer networks, data center operations, and other organizational stakeholders. The PSIRT defines privacy and security emergency situations, determines when such situations exist, and initiates appropriate countermeasures according to incident response procedures.

2. Terms of Reference for Privacy and Information Security Governance Framework

2.1. These terms of reference shall become effective as of the effective date of this EOI.

Purpose and Scope

2.2. The CISO, with broad inputs from organizational leaders, will provide advice to the ED and SLT on strategic planning and governance for all privacy and information security-related activities within UNOPS.

Objectives

2.3. The key objectives of the Privacy and Information Security Governance Framework are as follows:

- Direct the implementation of appropriate human resources, processes, and technologies to enable strong controls addressing privacy and information security risks.
- Evaluate and direct privacy and information plans and initiatives.
- Review and monitor conformance to privacy and information security obligations and performance.
- Develop organizational capabilities in privacy and information security.

2.4. Consequently accruing the following benefits for UNOPS:

- Strategic governance, risk management, and control of privacy and information security-related activities.
- Ensuring the processing of personal data is done in a rights-respecting manner and in adherence to established privacy principles (e.g., lawfulness, fairness, transparency, limitations on purpose, data minimization, accuracy of data, storage limitations, integrity, and confidentiality, and accountability).
- The availability, integrity, and confidentiality of UNOPS information assets are maintained throughout their life cycle.

Duties and Responsibilities

2.5. The CISO with organizational cross-function support shall:

- Ensure that the implementation of privacy and information security controls is coordinated across the organization.
- Identify and provide guidance on how to manage non-compliance with privacy and information security policies.
- Review and approve methodologies, processes, and technologies for privacy and information security.
- Ensure that Internal Audit and Investigations (IAIG) are consulted when implementing new or significant changes to financial or critical business information systems.
- Direct the preparation, review, and approval of the organization's disaster recovery plans that integrate with the agency's business continuity plan.
- Direct the preparation, review, and approval of the organization's information security awareness plan.
- Provide advice to the ED and SLT on developing privacy and information security capabilities within UNOPS.
- Provide guidance to the ED and SLT on emerging legal and regulatory developments that will impact privacy and information security.
- Embed 'privacy by design' and 'security by design' philosophies and best practices into business as usual.
- Promote information security education, awareness, and training across the organization.

Key Actions

2.6. The CISO shall provide advice to the ED and SLT on:

- Strategic alignment of privacy and information security in support of organizational goals.
- Management and mitigation of privacy and information security risks that impact the organization adversely.

- Optimal use of privacy and information security capabilities and resources (people, process, and technology) to deliver value to the organization and its overall mission.

Recommended Cross-Function Inputs

2.7. Inputs into the Privacy and Information Security Governance Framework should come from, but not be limited to, the following organizational leaders:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Financial Officer (CFO)
- Chief of Security
- HQ Directors
- Regional Directors

Accountability

2.8. The CISO as the overall custodian of the Privacy and Information Security Governance Framework shall act as an advisor.

2.9. Decisions shall be made by the ED and SLT.

3. Terms of Reference for PSIRT

3.1. These terms of reference shall become effective as of the effective date of this EOI.

Purpose and Scope

3.2. The Privacy and Security Incident Response Team (PSIRT) has been established to take responsibility for the prevention, identification, analysis, containment, and resolution of privacy computer/network security incidents. Privacy and security incidents are events that could compromise the privacy of UNOPS staff, personnel, and partners as well as adversely impact UNOPS computer or network resources and/or cause loss of or damage to electronic information resources.

Objectives

3.3. The key objectives of the PSIRT are as follows:

- Control and manage privacy and security incidents
- Timely investigation and assessment of the severity of the incident
- Timely recovery or bypass of the incident to normal operating conditions
- Timely notification of privacy breaches to data subjects
- Timely notification of serious incidents to the ED and SLT.
- The prevention of similar incidents in the future

3.4. Consequently accruing the following benefits for UNOPS:

- Damage from privacy and security incidents is minimized and controlled in an effective manner (damages can be operational, financial, reputational, etc. or a combination of various impact areas)
- Damage from privacy and security incidents is properly assessed and remediative actions are aligned with best practice and legal/regulatory requirements.

- Routine coordination between various departments and ownership of key processes and interfaces is established.
- Engagement with external actors such as law enforcement, media, insurance, etc. is effectively achieved.
- Lessons learned are properly integrated into the control framework and future response processes.

Duties and Responsibilities

3.5. The PSIRT shall:

- Maintain availability for 24x7 communication access and incident response
- Develop and maintain incident classification scheme
- Monitor UNOPS reporting mechanisms for indications of incidents
- Notify and consult with the SLT
- Assess scope of incident damage
- Classify incidents by severity
- Determine if incident can be investigated
- Control and contain incident
- Collect, document and preserve incident evidence
- Maintain chain of custody of all incident evidence
- Interview individuals involved in incident
- Conduct investigation to identify incident root cause or source, extent of damage, and recommended countermeasures
- Coordinate release of information with Communications team (internally and externally)
- Consult with law enforcement agencies, as authorized
- Follow all policies, laws, and regulations relating to privacy and security
- Prepare reports describing incident investigations
- Prepare recommendations to prevent future similar incidents
- Prepare recommendations to resolve incident and/or reduce impact of incident
- Prepare recommendations to bypass or remedy conditions leading to incident
- Monitor recovery
- Identify CSIRT operational improvements
- Assist recovery from incident, where applicable

Composition of Team

3.6. The following functions/departments should be involved in an incident:

- Information Security
- ICT
- Finance
- People and Change Group
- Security & Safety
- Legal
- Communications
- Internal Audit
- Regions

There are no permanent members of the PSIRT with the exception of the Chair. Heads of departments will nominate key interfaces for the PSIRT. The PSIRT is not a standing body, and only convenes as a cross-functional mechanism to effectively manage privacy and security incidents to completion.

PSIRT - Chair

3.7. The Chief Information Security Officer (CISO) acts as PSIRT Chair. The chair approves initiation of a PSIRT investigation and PSIRT activities performed in support of the investigation. Responsibilities include:

- Convene PSIRT
- Conduct PSIRT meetings
- Coordinate PSIRT investigation
- Ensure incidents are classified according to severity class
- Determine investigation objectives
- Define/obtain resource requirements
- Communicate with external agencies
- Coordinate PSIRT training and exercises
- Prepare post-mortem "Lessons Learned" analysis
- Request support team resources
- Prepare PSIRT management reports
- Consult with the SLT on incidents classified with a moderate or high severity rating
- Communicate with department manager(s) regarding incident investigation status
- Arrange for responsibility coverage during temporary absences

PSIRT Training

3.8. PSIRT team members are required to obtain training and periodic updates in the following knowledge and skill areas:

- Appropriate national, regional, and international laws
- UNOPS policies, standards, and guidelines
- Investigative processes
- Evidence handling and protection
- Technical PSIRT hardware and software tools

PSIRT Exercises

3.9. The PSIRT will conduct an annual exercise that simulates privacy and security incidents. The purpose of the exercise will be to maintain the skills and knowledge of PSIRT members. The exercises will involve all PSIRT team members. At the end of the exercise, the PSIRT Chair will prepare a brief report to the SLT evaluating the exercise. Any skill and/or knowledge area that needs to be improved as well as procedural enhancements will be identified in the report.loitation, abuse, and harassment, in a manner proportional to their size and risk profile.

Incident Definition

3.10. For the purposes of this document, an incident is defined as an event that has actual or potential adverse effects on individual privacy or computer and network resources resulting in misuse or abuse, compromise of information, or loss or damage of property or information. Any such events that originate from, are directed towards, or transit UNOPS controlled facilities, systems or network resources will fall under the purview of PSIRT. This definition is purposely made inclusive, however it is foreseen that many events classified with a "limited" severity rating may be handled by semi-

automated means and not require any further escalation. Incident types include, but are not limited to: Compromised Machine, Laptop Lost or Stolen, Denial of Service, Hoax, Malicious Code, Policy Violation, Probe, Unauthorized Access, Unauthorized Use.

Incident Reporting

3.11. All UNOPS employees shall report any potential event that adversely impacts the Confidentiality, Integrity, or Availability of Institutional Information, regardless of form (paper or electronic), Infrastructure Technology, or Information Systems by email (ciso@unops.org[1]). An incident shall also be immediately reported through the Privacy and Security Incident Reporting Form (online form). In addition, the PSIRT Chair will coordinate with all relevant departments to ensure that PSIRT is notified of any reported problem that may reflect a security incident. The individual reporting the incident will be asked to provide date, time, time zone, user contact information, brief description of the incident, and other pertinent information. Acknowledgement of a reported incident by the PSIRT shall occur via an auto-generated response to email. A telephone-reported incident will be acknowledged with a telephone call or email message from the PSIRT. All user reports will be analyzed, classified by severity rating, and an appropriate response will be generated. The scope of PSIRT response will be determined by the incident severity rating, or as directed by the ED and SLT. If the nature of the incident cannot be reported via non-confidential methods, the incident may be directly reported to the CISO.

Incident Classification and Prioritization

3.12. Incidents will be analyzed and the severity of the incident classified according to several factors. As a guide, the overall severity classification of an incident will be higher based on the critical nature of the targeted system for the organization, the type and quantity of data impacted and broad negative organization and user impact of the incident. The overall severity classification of an incident will be reduced when there are readily available alternatives to remedy or bypass the problem situation. Severity ratings will be labeled as low, medium, or high. The PSIRT will use the following table as a guideline in establishing incident severity.

Incident Factors	**Severity Factors**		
	Low	**Medium**	**High**
Criticality-Privacy	Individuals either will not be affected or encounter few inconveniences	Individuals may encounter significant inconveniences, which they will be able to overcome	Individuals may encounter significant, or even irreversible consequences, which they may not be able to overcome
Criticality-Application	Non-business critical application	Business critical application limited scope	Business critical UNOPS wide
Criticality-Infrastructure	No	Limited Scope	UNOPS wide

1. mailto:ciso@unops.org

Impact-User/ System	Affects a few people or a few systems	Department-wide impact	UNOPS wide impact
Impact-Public	None	Potential impact	Likely impact
Countermeasures	Solutions are readily available	Weak countermeasures	No countermeasures
Resolution procedures	Available and well-defined	Resolution procedures not well-defined	No resolution procedures available

3.13. Incidents receiving a "**high**" severity classification will receive the highest priority of PSIRT resources. In the case of multiple incidents, the higher severity rating incidents will receive higher priority PSIRT work assignment. The incident severity classification will also determine the degree of involvement of senior managers in respect to the incident investigation. **Medium** severity incidents may involve consultation with the CISO. **High** severity incidents will always involve consultation with the CISO, CIO, and CFO.