2. Monitoring and Responding to Security Events or Incidents

Security monitoring in Information and Cybersecurity Division mainly focuses on ensuring that information gathered and collected from the Security Operations Center and other reporting parties are identified and evaluated for relevancy, documented, and escalated. As the Security Monitoring Unit identifies and evaluates information gathered for relevance, security events are documented and escalated as needed. This whole process is summed up into four major stages: Detection, Collection, Assessment and Decision, and lastly, Reporting and Escalation.

Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the "incident"). Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum. This process covers the procedure of the Incident Response Unit's response to reported violations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" and other pertinent laws and standards about information security, incident response, and cybersecurity.

Office or Division:	Information and Cybersecurity Division
Classification:	Highly Technical
Type of Transaction:	G2G – Government to Government
Who may avail:	PRO Assets and System Owners/ PRO Officials and Employees

CHECKLIST OF REQUIREMENTS	WHERE TO SECURE
Security Event Report Form	Security Event Monitoring Matrix

CLIENT STEPS	AGENCY ACTIONS	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE
1. Accomplish and send the Security Event Report Form (SERF).	1.1. Acknowledge the accomplished SERF.	None	30 minutes	PRO-SOC Focal Persons of each division *Information Systems Analyst III* Security Monitoring Unit
None	1.2. Acknowledge the Security Event Monitoring Matrix	None	15 minutes	*Information Systems Analyst III*

	(SEMM) ticket created by the submitted SERF.			Security Monitoring Unit
None	1.3. Conduct Event Validation, Evaluation, and Confirmation (VEC) process.	None	1 day	*Information Systems Analyst III* Security Monitoring Unit *Information Systems Analyst II/I* Security Monitoring Unit
None	1.4. Prepare and submit Security Monitoring Unit Initial Assessment Form (SIAF) for approval	None	1 day	*Information Systems Analyst II/I* Security Monitoring Unit
None	1.5. Review and provide a decision based on the submitted SIAF **Note:** Revise as needed.	None	3 hours	*Information Technology Officer III/II* *Information Systems Analyst III*
None	1.6. Provide the status of the event through the SEMM. **Note:** If the event is not considered as a security threat, inform the client. If the event is considered as a security threat, proceed to the next step. Otherwise, end of the process.	None	30 minutes **Note:** Total time from receiving the SERF to responding to the Client should be within 24 hours.	*Information Systems Analyst II/I* Security Monitoring Unit
None	1.7. Receive the call/email and check SEMM.	None	15 minutes	*Information System Analyst III* Incident Response Unit

None	1.8. Verify and generate the initial report in SEMM.	None	15 minutes	*Information System Analyst II/I* Incident Response Unit
None	1.9. Prepare the Incident Initial Assessment Form (IIAF).	None	4 hours	*Information Technology Officer III/II* First Respond Team *Information System Analyst III/II/I* Incident Response Unit
2. Provide information regarding the incident.	2.1. Interview the incident reporter (client).	None	1 hour	*Information System Analyst II/II/I* Incident Response Unit
None	2.2. Respond to the security incident mentioned in the initial assessment report.	None	30 minutes **Note:** If within PRO Premises	*Information System Analyst II/II/I* Incident Response Unit
None	2.3. Isolate the affected/ compromised machines and secure the area.	None	30 minutes	*Information System Analyst I* Incident Response Unit
None	2.4. Investigate and perform forensic analysis.	None	1 day **Note:** Depending on the severity of the incident)	*Information System Analyst III/II/I* Incident Response Unit
None	2.5. Provide instructions and precautionary measures to the incident reporter (client).	None	1 hour	*Information System Analyst III/ II* Incident Response Unit

None	2.6. Acquire evidence such as data, memory, etc.	None	2 days **Note:** Depending on the severity of the incident	*Information System Analyst II/I* Incident Response Unit
None	2.7. Assess the collected evidence.	None	1 day **Note:** Depending on the severity of the incident	*Information System Analyst III/II/I* Incident Response Unit
None	2.8. Create and submit a complete incident final assessment report.	None	4 hours	*Information System Analyst III/II/I* Incident Response Unit
None	2.9. Escalate to ISMD with recommendation/s.	None	15 minutes	*Information Technology Officer III/II* Data Breach Response Team *Information System Analyst III/II/I* Incident Response Unit
None	2.10. Assist with ISMD during response action until resolved.	None	6 days **Note:** Depending on the severity of the incident	ISMD Personnel *Information System Analyst III/II/I* Incident Response Unit
None	2.11. Prepare a complete detailed documentation of the incident.	None	1 hour	*Information System Analyst III/II/I* Incident Response Unit
None	2.12. Review and signature of the documentation of the	None	1 day	*Information System Analyst III*

	incident by the ICD Division Chief and SISS Assistant National Statistician.		**Note:** Depending on the time of the concerned personnel	Incident Response Unit ICD Division Chief Assistant Division Chief SISS Assistant National Statistician
None	2.13. Submit the signed documentation of the incident to SMU will close the ticket.	None	15 minutes	*Information System Analyst* II/ I Incident Response Unit *Information System Analyst* II/I SMU Unit
3. Attend a cybersecurity awareness seminar.	3.1. Review the incident response documented procedures in coordination with personnel/s involved and take preventive steps so the intrusion cannot happen.	None	1 day	DBRT *Information System Analyst* III/II/I Incident Response Unit Reporter/ involved personnel
	TOTAL:	**None**	**16 days and 15 minutes**	