



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF AGRICULTURE
BUREAU OF AGRICULTURAL RESEARCH
RDMIC Bldg., Elliptical Road corner Visayas Avenue, Diliman, Quezon City 1104
(+632) 8461 2800 and (+632) 8461 2900 • r4d@bar.gov.ph

Reference No. 2024- 166
August 5, 2024

MEMORANDUM FOR THE DIRECTOR

FROM : SALVACION M. RITUAL
Data Protection Officer / Chair, Data Breach Response Team

**SUBJECT : ENDORSEMENT OF THE PROPOSED SECURITY INCIDENT
MANAGEMENT POLICY**

Please find the attached Data Breach Response Team (DBRT) resolution endorsing and committing to the implementation of the security incident management policy.

The DBRT recognizes the critical importance of a comprehensive SIMP in safeguarding the agency's sensitive agricultural research data and information, including personal data as defined under Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012. The proposed SIMP aligns with the requirements of the Data Privacy Act and provides a robust framework for addressing security incidents, including data breaches.

We are confident that the proposed SIMP will significantly enhance the agency's ability to respond effectively to security incidents and minimize potential damages.

For information and further instructions.

NOTED BY:

JUVEL B. SORIANO, PhD
Director



BAGONG PILIPINAS



Magandang Agrikultura,
Masagana at Masaya

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF AGRICULTURE
BUREAU OF AGRICULTURAL RESEARCH
RDMC Bldg., Elliptical Road corner Visayas Avenue, Diliman, Quezon City 1104
(+632) 8461 2800 and (+632) 8461 2900 • 14a@bar.gov.ph

**DEPARTMENT OF AGRICULTURE
BUREAU OF AGRICULTURAL RESEARCH
MANAGEMENT COMMITTEE**

RESOLUTION NO. ____
Series of 2024

**RESOLUTION RECOMMENDING THE APPROVAL OF THE
PROPOSED SECURITY INCIDENT MANAGEMENT POLICY**

WHEREAS, Article XIV Section 10 of the 1987 Constitution of the Republic of the Philippines, emphasizes that science and technology are essential for national development and progress, prioritizing research and development, invention, innovation, and their utilization, along with science and technology education, training, and services;

WHEREAS, Executive Orders 292 and 116 (Series of 1987) established the Department of Agriculture-Bureau of Agricultural Research (DA-BAR) and tasked it with coordinating and conducting agricultural research for maximum benefit;

WHEREAS, the DA-BAR is entrusted with sensitive agricultural research data and information critical to food security and national development, as well as personal information of its employees, partners, and other stakeholders;

WHEREAS, the increasing frequency and sophistication of cyber threats pose significant risks to the agency's operations, data integrity, and overall security;

WHEREAS, a comprehensive Security Incident Management Policy is essential to protect the agency's assets, ensure business continuity, and comply with relevant laws and regulations;

WHEREAS, the Data Privacy Act of 2012 mandates the protection of individual privacy in information and communications systems;

WHEREAS, the proposed Security Incident Management Policy aligns with the data privacy principles of transparency, accountability, and security as enshrined in the Data Privacy Act;

WHEREAS, the policy incorporates measures to protect personal data from unauthorized access, loss, or destruction, in compliance with the law;

WHEREAS, the policy outlines procedures for notifying the National Privacy Commission and affected individuals in case of a data breach, as required by law;

WHEREAS, the policy recognizes and respects the rights of data subjects to access, rectify, block, or erase their personal data;

Y



(Resolution recommending the approval of the proposed DA-BAR Security Incident Management Policy)

NOW, THEREFORE, BE IT RESOLVED, as it is hereby resolved, by the Management Committee of the DA-BAR to recommend the approval of the proposed Security Incident Management Policy;

BE IT FURTHER RESOLVED, that upon approval by the appropriate authority, the Security Incident Management Policy shall be implemented and disseminated to all DA-BAR personnel;

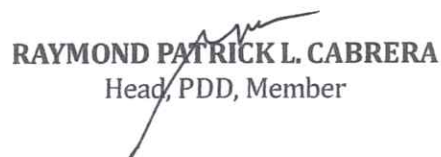
BE IT FURTHER RESOLVED, that the Management Committee shall regularly review and update the policy to address emerging threats and technological advancements.

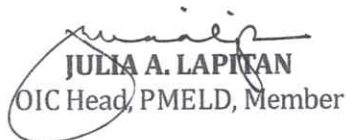
APPROVED, CONFIRMED AND SIGNED by the DA-BAR Management Committee Chair and Members via Ad referendum this August 2, 2024.


JOELL H. LALES
Assistant Director, Member


GIAN CARLO R. ESPIRITU
Head, PMU, Member


MELISSA A. RESMA
Compliance Officer, Member

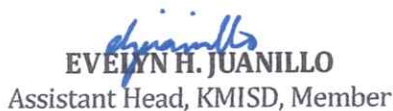

RAYMOND PATRICK L. CABRERA
Head, PDD, Member


JULIA A. LAPITAN
OIC Head, PMELD, Member


SALVACION M. RITUAL
Head, KMISD, Member


KRIS THEA MARIE B. HERNANDEZ
OIC Assistant Head, PDD, Member


AMAVEL A. VELASCO
OIC Assistant Head, PMELD, Member


EVELYN H. JUANILLO
Assistant Head, KMISD, Member



ALVIN L. FONTANIL
Section Head, PPES, Member


ETHCEL PRINCESS P. LIBANG
Section Head, TMS, Member


MARJORIE M. MOSENDE
Section Head, IDS, Member





(Resolution recommending the approval of the proposed DA-BAR Security Incident Management Policy)



ERIC J. MORALES
OIC Section Head, RMS, Member


RHEA D. DESALESA
Section Head, RLS, Member

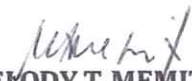

MARIA ELENA M. GARCÉS
Section Head, SLSS, Member


MA. FLOISA H. AQUINO
OIC Section Head, ACS, Member


JOCEL ANNE C. YAMSON
OIC Section Head, IMS, Member

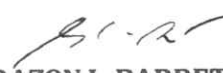

JUDE RAY P. LAGUNA
OIC Head, AFD/Head, HRMU, Member


ROBERTO S. QUING, JR.
OIC Asst. Head, AFD/Head, AU, Member


MELODY T. MEMITA
Unit Head, RU and BMSGUSU, Member


JUDITH A. MAGHANOY
Unit Head, PU, Member


MARILOU C. OREN
Unit Head, BU, Member


CORAZON L. BARRETTO
Unit Head, SPU, Member


GRETEL F. RIVERA
Unit Head, CU, Member


JENNIFER T. ALIANZA
Unit Head, TMSU, Member


APPROVED/DISAPPROVED:


JUNEL B. SORIANO, PhD
Director



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF AGRICULTURE
BUREAU OF AGRICULTURAL RESEARCH
RDMC Bldg., Elliptical Road corner Visayas Avenue, Diliman, Quezon City 1104
(+632) 8461 2800 and (+632) 8461 2900 • 14d@bar.gov.ph

**DEPARTMENT OF AGRICULTURE
BUREAU OF AGRICULTURAL RESEARCH
DATA BREACH RESPONSE TEAM**

RESOLUTION NO. 1
Series of 2024

**RESOLUTION ENDORSING AND COMMITTING TO THE
IMPLEMENTATION OF THE SECURITY INCIDENT MANAGEMENT POLICY**

WHEREAS, the Department of Agriculture – Bureau of Agricultural Research (DA-BAR) is a government agency entrusted with handling sensitive agricultural research data and information, which includes personal data as defined under Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;

WHEREAS, the Data Privacy Act mandates the protection of individual privacy in information and communications systems, emphasizing the importance of safeguarding personal data;

WHEREAS, the increasing sophistication of cyber threats necessitates a robust framework for managing security incidents to protect the rights of data subjects and ensure compliance with the Data Privacy Act;

WHEREAS, the proposed Security Incident Management Policy was developed in accordance with the principles and requirements of the Data Privacy Act, providing a comprehensive and systematic approach to addressing security incidents, including data breaches;

WHEREAS, the Data Breach Response Team is committed to safeguarding the agency's data, protecting the rights of data subjects, and ensuring compliance with the Data Privacy Act;

NOW, THEREFORE, BE IT RESOLVED, as it is hereby resolved, by the Data Breach Response Team of the DA-BAR to fully endorse the proposed Security Incident Management Policy as a crucial step towards fulfilling the agency's obligations under the Data Privacy Act;

BE IT FURTHER RESOLVED, that the Data Breach Response Team shall actively participate in developing and updating standard operating procedures based on the policy to ensure effective response to security incidents and compliance with data privacy requirements;

BE IT FURTHER RESOLVED, that the Team shall conduct regular training and simulations to enhance its capabilities in incident response, with a particular focus on data privacy principles and practices;

Y

(Resolution endorsing and committing to the implementation of DA-BAR Security Incident Management Policy)

BE IT FURTHER RESOLVED, that the Team shall conduct post-incident reviews to identify lessons learned and recommend improvements to the Security Incident Management Policy, taking into account the requirements of the Data Privacy Act.

APPROVED, CONFIRMED AND SIGNED by the DA-BAR Data Breach Response Team Chair and Members this August 2, 2024.


SALVACION M. RITUAL
Chair


EVELYN H. JUANILLO
Vice Chair


RAYMOND PATRICK L. CABRERA
Member


JULIA A. LAPITAN
Member


JUDE RAY P. LAGUNA
Member


ATTY. CHARMAINE V. CAYABAN
Member



SPECIAL ORDER

No. 243

Series of 2024

SUBJECT : CREATION OF THE DA-BAR DATA BREACH RESPONSE TEAM

In the interest of service and to ensure that the bureau is equipped with necessary knowledge on protocols and mitigation measures in the face of security and data threats, the DA-BAR Data Breach Response Team is hereby created, as follows:

- Chair :** **SALVACION M. RITUAL**
Head, Knowledge Management and Information Systems Division (KMISD)
- Vice Chair :** **EVELYN H. JUANILLO**
Asst. Head, Knowledge Management and Information Systems Division (KMISD)
- Members :** **RAYMOND PATRICK L. CABRERA**
Head, Program Development Division
- JULIA A. LAPITAN**
Head, Program Monitoring and Evaluation Division
- JUDE RAY P. LAGUNA**
OIC-Head, Administrative and Finance Division
- ATTY. CHARMAINE V. CAYABAN**
Development Management Officer IV, Office of the Director
- Secretariat :** **JOCEL ANNE C. YAMSON**
OIC-Head, KMISD-Information Management Section (IMS)
- JEMS RAY Y. SOTO**
Computer Programmer III, KMISD-IMS

As such they shall perform the following functions:

1. Spearhead the crafting and implementation of a security incident management policy;

2. Initiate crisis management on security and personal data breach incidents, including but not limited to:
 - a. Assessment and evaluation of security incidents;
 - b. Mitigation and recommendation of remedies on possible damages;
 - c. Compliance with necessary documentation requirements and packaging of official report to oversight; and,
3. Ensure the bureau's compliance with the Data Privacy Act and other related issuances from the National Privacy Commission.

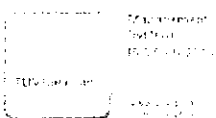
All divisions and units are hereby directed to extend full support and cooperation at all times to the team as may be necessitated along the course of their duties.

All expenses to be incurred in relation to this Order shall be charged against BAR funds subject to existing accounting and auditing rules and regulations.

This order shall take effect immediately, shall supersede all other Orders inconsistent herewith, and shall remain in force until revoked in writing.

Done this 17th day of **July 2024**.


JUNEL B. SORIANO, PhD
Director



(02) 8461 2860 | 8461 2900
r4a@bar.gov.ph
www.bar.gov.ph
DABAROfficial

Food-secure and resilient Philippines
with empowered and prosperous farmers and fisherfolk





REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF AGRICULTURE
BUREAU OF AGRICULTURAL RESEARCH
RDMIC Bldg., Elliptical Road corner Visayas Avenue, Diliman, Quezon City 1104
(+632) 8461 2800 and (+632) 8461 2900 • r4d@bar.gov.ph

SECURITY INCIDENT MANAGEMENT POLICY

Background

Republic Act No. 10173, or the Data Privacy Act of 2012 (DPA), states that it is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The law requires the adoption of a Security Incident Management Policy to prevent or minimize the risks imposed by data breaches and other security incidents. These include protocols to notify the National Privacy Commission (NPC) and affected individuals of data breaches under certain circumstances.

The Department of Agriculture - Bureau of Agricultural Research recognizes the importance of data privacy and data protection. Hence, it is imperative that the Bureau is prepared and has the necessary protocols to facilitate the proper handling of data breaches and other security incidents in order to minimize their impact and ensure compliance with all applicable laws and policies.

1. Objective

This policy is promulgated to:

- Establish a security incident response team and define its roles and responsibilities.
- Ensure security incidents, including data breaches, are handled in a timely manner, properly investigated and handled in accordance with the response procedures to contain a security incident.
- Ensure the availability, integrity and confidentiality of the Personal Data being processed through its information and communication system.

2. Purpose

The purpose of this Security Incident Management Policy, hereinafter referred to as "Policy" is to establish a systematic approach for identifying, managing, and responding to security incidents that may impact the confidentiality, integrity, and availability of information systems and data within the organization. This policy aims to ensure timely and effective resolution of security incidents to minimize potential damage and reduce risk.



3. Scope

The Policy applies to all employees, contractors, vendors, and other stakeholders who have access to the organization's information systems and data, including but not limited to hardware, software, networks, and facilities within the Philippines.

The Policy shall also cover all security incidents involving any data processing system of the Bureau and/or personal data under its control or custody.

4. Definition of Terms

- 4.1. **"Bureau"** refers to the Department of Agriculture - Bureau of Agricultural Research.
- 4.2. **"Data Processing Systems"** refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.
- 4.3. **"Data Protection Officer"** refers to the designated individual or individuals of the Bureau in accordance with NPC Advisory No. 2017-01, who shall be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security.
- 4.4. **"Data Subject"** refers to an individual whose personal, sensitive personal, or privileged information is processed.
- 4.5. **"Incident Response Team" or "IRT"** - refers to a designated group of individuals responsible for managing and responding to security incidents.
- 4.6. **"Personal Data Breach"** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
- 4.7. **"Personal Information"** refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information



would directly verify the identity of an individual.

4.8. “Personal information controller (PIC)” refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.

4.9. “Processing” refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system.

4.10. “Process Owner” refers to the office that owns, administers, and/or manages a data processing system, the principal custodian of a particular personal data under control or custody of the Bureau. It excludes offices or units of service providers.

4.11. “Profiling” refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

4.12. “Privileged information” refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged



communication.

4.13. "Security incident" refers to any event that comprises the confidentiality, integrity, or availability of information systems and data. This includes, but is not limited to, unauthorized access, data breaches, malware attacks, and denial of service (DoS) attacks;

4.14. "Sensitive Personal Information" refers to personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an executive order or an act of Congress to be kept classified.

5. Incident Response Team

An Incident Response Team (IRT) shall be created, which shall be responsible for investigating suspected security incidents.

The IRT shall be headed by the Data Protection Officers appointed by the Bureau. The members of the IRT include the head of the Program Development Division, the head of the Program Monitoring and Evaluation Division, and the head of the Administrative and Finance Division. Other members may be called on to join the IRT on a per-incident basis when their expertise is needed to adequately address the incident, as recommended by the permanent members.

Where a member of the IRT is the Process Owner involved in a reported incident, the Director of the Bureau shall designate a competent alternate. A service provider or external party may also be considered.



5.1. Assignment of Duties and Responsibilities

To ensure the effective implementation of this Policy, the following offices and individuals shall perform their respective functions and responsibilities:

5.1.1. IRT

- 5.1.1.1. Implementation of the Security Incident Management Policy of the personal information controller or personal information processor.
- 5.1.1.2. Management of security incidents and personal data breaches.
- 5.1.1.3. Ensure compliance by the personal information controller or personal information processor with the relevant provisions of the Data Privacy Act of 2012, its IRR, and all related issuances by the Commission on personal data breach management.
- 5.1.1.4. Investigate and assess suspected security incidents in coordination with all concerned divisions and units of the Bureau.
- 5.1.1.5. Recommend remedial measures to be performed by the Process Owner and other concerned divisions and units of the Bureau in relation to any suspected security incident.
- 5.1.1.6. Classify incidents based on their severity and impact on the Bureau.
- 5.1.1.7. Restoration of integrity to the information and communications system.
- 5.1.1.8. Mitigate and remedy any resulting damage.
- 5.1.1.9. Comply with reporting requirements as provided under the Data Privacy Act of 2012..

6. Notification of the DPO

Incident notification shall be carried out in accordance with the provision of this Section:

6.1. Subject of a Notification

An incident must involve a data processing system of the Bureau or personal data under the control and custody of the Bureau. It includes those being processed by a service provider or any other authorized third party.



6.2. Notifying Party and Recipient of Notification

Any person who becomes aware of or has reason to believe that an incident described by the previous subsection has occurred must notify the Data Protection Officer using the latter's contact information. If a notification is sent to or received by a different office of the Bureau, it shall be immediately referred to the DPO.

6.3. Method of Notification

Any person, whether connected with the Bureau or not, should report through email and/or phone call to the Data Protection Officer, immediately or within 24 hours from discovery of the incident or Personal Data Breach.

7. Investigation of Incidents

Investigations of incidents shall be carried out in accordance with the provisions of this Section:

- 7.1.** The DPO shall refer a reported incident to the concerned Process Owner. It shall also give advance notice to the IRT about the reported incident.
- 7.2.** Once informed by the DPO, the Process Owner shall accomplish an Incident Report and submit the same to the DPO within 24 hours. The Process Owner must inform the DPO before the expiration of such period if it requires additional time for addressing and/or investigation. However, in no case shall such additional time exceed five (5) calendar days. Whenever possible, the person/s who may be involved in the reported incident should not be made to accomplish the Incident Report to minimize any conflict of interest. The DPO shall not accept Incident Reports that are incomplete or improperly accomplished.
- 7.3.** The DPO shall refer the Incident Report to the members of the IRT for their evaluation. At this point, the IRT will determine if additional members are necessary to investigate the reported incident. If so deemed necessary, the IRT shall recommend the designation of additional members to the Director.



- 7.4. The IRT shall conduct its investigation of the incident based primarily on the Incident Report. However, it is not bound by such report and can perform any of the following tasks:
- 7.4.1. Direct clarificatory or follow-up questions to the Process Owner.
 - 7.4.2. Require additional submissions from the Process Owner.
 - 7.4.3. Request for a meeting with the Process Owner and other concerned offices of the Bureau, including individuals affected by the suspected security incident
 - 7.4.4. Perform other actions to obtain information critical to the investigation

The IRT shall complete its investigation within forty-eight (48) hours after it has obtained all information it needs to carry out its investigation. If it requires additional time, it must at least determine within this period whether or not a data breach has occurred, and if notification of the NPC is necessary. This initial assessment shall be relayed to the Director by the DPO.

- 7.5. The results of the investigation by the IRT shall be consolidated by the DPO into an IRT Assessment Report. The DPO may already advise the Process Owner regarding any initial or urgent recommendations by the IRT.
- 7.6. The IRT Assessment Report, together with the Incident Report and other relevant attachments, shall be recorded and stored in accordance with this Policy. However, if it contains recommendations and/or other matters that require the attention of or action from the Director, it shall be transmitted immediately to the latter for appropriate action.

8. Data Breach Notification to the NPC and to Data Subject

Notification of the NPC and affected data subjects shall be carried out in accordance with the provisions of this Section:

- 8.1. A confirmed data breach shall be reported to the NPC, if the Director, after being informed of the advice of the IRT, has determined that it meets all of the following conditions:
- 8.1.1. It involves sensitive personal information or any other information that may be used to enable identity fraud;
 - 8.1.2. There is reason to believe that the information may have been acquired by an unauthorized person; and
 - 8.1.3. There is reason to believe that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.



- 8.2.** If there is uncertainty regarding the need to notify the NPC, the following additional factors shall be considered by the Director and the IRT:
- 8.2.1.** Notification could reduce the risks arising from the data breach.
 - 8.2.2.** The data breach would likely affect national security, public safety, public order, or public health.
 - 8.2.3.** The personal data involved is required by applicable laws or rules to be confidential.
 - 8.2.4.** The personal data involved belongs or refers to vulnerable groups.
 - 8.2.5.** The data breach affects at least one hundred (100) individuals.
- 8.3.** The Director, with the assistance of the DPO and the IRT, shall notify the NPC within seventy-two (72) hours after he has determined that a confirmed data breach meets the conditions set out in Subsections 7.1 and/or 7.2 hereof.

For this purpose, the DPO shall send a notification letter to the NPC via email, as signed by the Director. The DPO shall make sure to obtain a confirmation from the NPC that it has received the notification letter. If online access is not available, the DPO shall personally deliver the notification letter to the NPC and maintain a receiving copy.

- 8.4.** There shall be no delay in notifying the NPC except in instances expressly allowed or recognized by the Commission through its Circular 16-03 and other applicable policies.
- 8.5.** The PIC must also notify affected individuals within the same period, unless there are grounds recognized by law that allow the Bureau to forgo such notification.

In determining whether a valid reason exists for not notifying affected individuals, the Bureau, through the IRT or the Director, may consult with the NPC.

- 8.6.** Whenever possible, the Bureau, through the concerned Process Owner, shall coordinate with all affected data subjects and provide appropriate guidance or assistance.



9. Reports and Documentation

All reported incidents shall be properly documented. The DPO shall develop forms for this purpose, facilitate their accomplishment by the responsible parties, and see to their secure storage and disposal. As a security measure, soft copies of all reports and related documents must be password-protected. Only those directly involved in their preparation and use shall have access to these documents.

10. Undertaking of Confidentiality

All information generated by or involved in the handling of security incidents shall be kept confidential by all concerned Parties. For this purpose, all Bureau Personnel involved must have accomplished the Non-Disclosure Agreement prescribed by the DPO before they assume their functions under this Policy.

Any public pronouncements involving such incidents must be coordinated with the DPO and shall be subject to the approval of the Director.

11. Remedial and Prevention Measures

To help prevent or avoid the same type of security incident from occurring, the following measures may be undertaken:

- 11.1.** The DPO may facilitate a debriefing session with the concerned Process Owner to ensure that remedial or preventive measures are properly implemented. It may also conduct an orientation regarding data privacy and compliance with the DPA.
- 11.2.** The IRT may recommend the conduct of a Privacy Impact Assessment (PIA) on the data processing system involved in a security incident, or on the entire office of the Process Owner. The DPO shall issue the necessary guidelines for the proper conduct of a PIA.
- 11.3.** The concerned Process Owner shall implement new security measures, and/or make changes to existing ones.
- 11.4.** The DPO, PIC, and concerned Process Owner, with guidance from the IRT, shall be responsible to contain the security incident so that it does not spread and cause further damage. Steps that may be taken are:



- 11.4.1.** Disconnect the affected devices from the internet or intranet
- 11.4.2.** Commence short-term and long-term strategies
- 11.4.3.** Ensure that there is a back-up systems to help us in the restoration process
- 11.4.4.** Update and patch the system
- 11.4.5.** Review remote access protocol
- 11.4.6.** Change user and administrative access credentials
- 11.4.7.** Secure passwords

12. Recovery

In coordination with the relevant Information and Communications Technology (ICT) DA-BAR Personnel, the DPO, PIC, Process Owner concerned and the IRT shall exert utmost effort to restore the system or application to a working state and take necessary actions to recover affected records, systems and other matters affected by the incident. The following tasks may be conducted:

- 12.1.** Restoring system data to its previous state
- 12.2.** Repairing and rebuilding of the affected/compromised system or application
- 12.3.** Validating if the problem that caused the incident has been fully addressed
- 12.4.** Communicating to users upon restoration of the affected/compromised system
- 12.5.** Disclosure of the incident to all affected users, if necessary
- 12.6.** Taking any appropriate administrative actions to address the incident

13. Penalties

Failure to comply with this Policy may result in disciplinary action, in accordance with the applicable Code of Discipline, and other relevant rules and regulations. DA-BAR reserves the right to exercise any/other legal remedies available to it, such as, but not limited to applicable laws, policies, rules and regulations.



14. Review

This Policy shall be amended and updated every two (2) years, unless special circumstances require earlier modifications/revisions, or to comply with new and existing relevant DPA laws, rules, regulations and issuances by the NPC.

15. Effectivity

Upon approval by the Data Breach Committee, this Policy and any subsequent amendment thereto shall take effect immediately after it has been posted in the Bureau's Official Website

APPROVED BY:



SALVACION M. RITUAL
Chair, Data Breach Response Team
Data Protection Officer

