DATA PRIVACY MANUAL

_____, MD

[DATE]

TABLE OF CONTENTS

PRIVACY MANAGEMENT PROGRAM (PMP)

Organizational Commitment

I, _____, MD, acknowledge that my medical practice must comply with the Data Privacy Act (DPA) and related issuances by the National Privacy Commission (NPC), and further acknowledge my accountability for the protection of personal data under our control or custody.

This Privacy Management Program documents the control measures for privacy and data protection implemented in my clinic and puts in place a review system for assessment and continuous improvement of the program.

Accountable and Responsible Persons

As head attending physician, I, _____, MD, am the de facto Data Protection Officer (DPO) of this practice and am accountable for complying with the Data Privacy Act. As DPO, I shall:

1. Monitor compliance with the DPA, its Implementing Rules and Regulations (IRR), issuances by the NPC and other applicable laws and policies. For this purpose, he or she may maintain a record of processing activities;
2. Review the personal data flow to determine need of Data Sharing Agreements, outsourcing contracts, and privacy impact assessments. Review on a regular basis existing policies, guidelines, projects and programs in the clinic;
3. Address concerns of data subjects (e.g., requests for information, clarifications, rectification or deletion of personal data and serve as contact person and regularly coordinate with the National Privacy Commission;
4. Ensure proper data breach and security incident management, including compliance with reporting requirements; and
5. Cultivate privacy and data protection in the clinic.

All permanent and part-time employees, as well as contractual workers in my clinic are aware of the Data Privacy Act, and related issuances. They will all take necessary measures to:

1. Report to the DPO security incidents and personal data breaches;
2. Sufficiently address any concern from patients as data subjects;
3. And comply with the privacy policies and procedures in the clinic.

Reporting Mechanisms

The DPO shall document monitoring activities, risk assessments, and privacy related activities. This will include: DPA compliance activities, PIAs, audits and security assessments, breach management, complaints, the exercise of data subject rights, review processes and other means to evaluate effectiveness of the Privacy Management Program.

Program Controls

Records of Processing Activities

Records of processing activities are electronically recorded, time-stamped, and stored in our third party Electronics Medical Records (EMR) platform, **MedCheck EMR**.

Risk Assessment

Privacy impact assessment will be conducted on a yearly basis, or when there are new programs, projects and products, a change in law or regulation, or other changes within the clinic.

DPO shall continuously evaluate the effectiveness of security measures in the clinic.

Policies and Procedures

There are policies and procedures to govern the processing of personal data from collection to storage or disposal. These include policies and procedures for:

1. Adherence to Data Privacy Principles;
2. Implementation of security measures;
3. Means for data subjects to exercise their rights;
4. And documentation, review, and updating of the Privacy Management Program.

Security Measures

We implement organizational, physical and technical security measures to maintain the confidentiality, integrity and availability of personal data. Our EMR provider **MedCheck** also implements a high level of technological measures to maintain the security, confidentiality, integrity, and availability of personal data.

Capacity Building

Clinic personnel and I will attend any capacity building, orientation or training programs related to privacy and data protection at least once every year. To build knowledge on privacy and data protection, we will visit the website of the National Privacy Commission at least once per month. A copy of the NPC toolkit has been downloaded for reference for myself and clinic personnel.

Registration and Notification

Our clinic complies with reporting and notification requirements.

Breach Management

A Breach Management Program is in place, including personal data breach notification and annual report on breaches and security incident. This is contained in our Security Incident Policy.

Personal Information Processor and Third Party Management

There will be no transfers of personal data outside the clinic unless the Data Protection Officer has evaluated and approved such transfer.

Contracts with third party service providers shall be regularly reviewed to assure protection for personal data being processed by a third party. External consultants shall be engaged when necessary.

Communication

Our clinic maintains Privacy Notices. In case of change in privacy policies, the Privacy Notice will be updated.

A patient as data subject with any concerns related to privacy or data protection will be instructed to send an e-mail to the Data Protection Officer. Concerns will be addressed within ten (10) days, but may be longer if required by the situation. The data subjects will be informed in case the action on the concern will take longer.

Continuing Assessment and Development

As DPO, I will monitor data processing systems and ensure conduct of PIAs when necessary. Organization conducts and updates PIAs regularly, and when there are new programs, projects and products, a change in law or regulation, or other changes within the organization.

Privacy and security policies and practices in the clinic will be reviewed yearly, and updated when necessary.

The PMP shall be evaluated annually and revised as needed, taking into account Privacy Impact Assessments (PIAs), effectiveness of implementation, and data privacy best practices.

Our clinic monitors emerging technologies, new threats and risks to data processing systems, international data protection standards, and the legal and ICT environment through regular visits to the National Privacy Commission website, and through attendance in privacy workshops.

POLICIES AND PROCEDURES

Security Incident Policy

In order to manage security incidents, including personal data breach, our physicians and clinic personnel shall implement the following:

A. Organization, Physical and Technical measures shall to ensure confidentiality, integrity and availability of personal data in paper-based records. These shall include securing storage area of personal data, by use of lock and key. Physical access to storage area shall be restricted to healthcare provider and clinic personnel.

   Health Information Management System Providers (Service Providers) shall be required to implement security measures directed to ensuring the availability, integrity, and confidentiality of the personal data being processed, and may include: implementation of back-up solutions; access control and secure log files; encryption; and data disposal and return of assets policy.

B. Policies and procedures shall be regularly reviewed, including the testing, assessment, and evaluation of the effectiveness of the security measures.

C. All healthcare provider and clinic personnel shall on a daily basis monitor for security breaches involving paper-based records in their custody. Storage areas, locks, and other security measures shall be examined.

D. All healthcare provider and clinic personnel shall report any suspicion of a security incident or personal data breach to the designated Data Protection Officer.

   The report may be relayed verbally, but a written report containing the following information should be prepared:

   a. Date and Time of Report;
   b. Nature of the Security Incident or Personal Data Breach;
   c. Records affected, including number of data subjects affected;
   d. Nature of compromised personal data;
   e. Any actions taken upon discovery or suspicion that a security incident or personal data breach occurred;
   f. Any persons contacted, including notification of service provider, where applicable; and
   g. Information on whether a report had been made to law enforcement.

   Service Providers shall be required to notify the Data Protection Officer in case of knowledge or reasonable belief that a personal data breach occurred, within 24 hours from knowledge, based on available information.

E. The Data Protection Officer shall keep a record of all reported security incidents or personal data breach, including

   a. Date and Time of Report;
   b. Nature of the Security Incident or Personal Data Breach;

i. In case of a personal data breach, the description of the personal data breach, its root cause and circumstances regarding its discovery
ii. Records affected, including number of data subjects affected
iii. Nature of compromised personal data

c. Any action taken upon discovery or suspicion that a security incident or personal data breach occurred, including actions and decisions of the incident response procedure followed;
    i. Any persons contacted, including notification of service provider, where applicable
    ii. Information on whether a report had been made to law enforcement
d. Outcome of the breach management, and difficulties encountered; and
e. Compliance with notification requirements and assistance provided to affected data subjects, where applicable

The reports shall be summarized for yearly reporting to the National Privacy Commission.

Incident Response Procedure

A. The Data Protection Officer shall set in motion the incident response procedure.
B. The DPO shall assess and evaluate the security incident, mitigate and remedy any resulting damage, and comply with reporting requirements.
C. The DPO shall conduct a preliminary assessment for purpose of:
    a. Assessing, as far as practicable, the nature and scope of the personal data breach and the immediate damage;
    b. Determining the need for notification of law enforcement or external expertise; and
    c. Implementing immediate measures necessary to secure any evidence, contain the security incident and restore integrity to the information and communications system;
D. The DPO shall contact external expertise, where appropriate. The DPO, with or without assistance of external expertise, shall conduct investigations to evaluate fully the security incident or personal data breach.

Paper-based Records

i. An investigation will be commenced upon any report of suspicious activity, security incidents and personal data breaches.
ii. The involved healthcare provider or clinic personnel will be requested to provide an incident report.
iii. If there are reasons to believe that the personal data breach resulted due to criminal activity, law enforcement shall be notified.

Electronic Records

i. In case the security incident involves the HIMS, the DPO shall contact Service Provider or IT support to assess and evaluate a security incident, restore integrity to the information and communications system, mitigate and remedy any resulting damage.

ii. In case of knowledge or reasonable belief that a security breach has occurred, the service provider shall be immediately contacted. A requires for information on the security incident or personal data breach shall be required, which shall include: nature, extent and cause, the adequacy of safeguards in place, immediate and long-term damage, impact of the breach, and its potential harm and negative consequences to affected data subjects.

iii. The service provider shall be asked to contact law enforcement in case criminal activity is suspected.

E. In case of knowledge or reasonable belief that a personal data breach has occurred, the DPO shall notify the National Privacy Commission and Data Subjects. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that personal data breach requiring notification has occurred, under the following conditions:
    a. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. These shall include data about the financial or economic situation of the data subject; usernames, passwords, and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

Notification Requirements

Notification of the Data Privacy Commission

A. The DPO shall notify the Commission of a personal data breach within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or person information processor that a personal data breach has occurred, based on available information. The full report of the personal data breach shall be submitted within five (5) days, unless the DPO is granted additional time by the Commission to comply.
B. Content of Notification – the notification shall include (but not limited to):
    a. Nature of the Breach
        i. Description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
        ii. A chronology of the events leading up to the loss of control over the personal data;
        iii. Approximate number of data subjects or records involved;
        iv. Description or nature of the personal data breach
        v. Description of the likely consequences of the personal data breach; and
        vi. Name and contact details of the data protection officer or any other accountable persons.
    b. Personal Data Possibly Involved
        i. Description of the sensitive personal information involved; and
        ii. Description of other information involved that may be used to enable identity fraud.

c. Measures Taken to Address the Breach
    i. Description of the measures taken or proposed to be taken to address the breach;
    ii. Actions being taken to secure or recover the personal data that were compromised;
    iii. Actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
    iv. Action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification; and
    v. The measures being taken to prevent a recurrence of the incident.

C. The report to the National Privacy Commission shall be done by electronic mail, addressed to complaints@privacy.gov.ph. The DPO shall also contact the Privacy Commission to confirm receipt of notification.

Notification of Data Subjects

A. The DPO shall notify the data subjects affected by a personal data breach within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects.
B. Content of Notification – the notification shall include (but not limited to):
    a. Nature of the breach;
    b. Personal data possibly involved;
    c. Measures taken to address the breach;
    d. Measures taken to reduce the harm or negative consequences of the breach;
    e. Representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
    f. Any assistance to be provided to the affected data subjects.

    Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.

C. The DPO may request the Commission for an exemption from the notification requirement, or the postponement of the notification, for the following reasons:
    a. It is not reasonably possible to notify the data subjects within the prescribed period; or
    b. Notification would not be in the public interest or in the interest of the affected data subjects.
D. Where individual notification is not possible or would require a disproportionate effort, the DPO may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure.
E. The DPO shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach. The Healthcare providers shall also provide assistance to data subjects whose personal data may have been compromised.

Post-Breach Review

A. A post-breach review will be conducted in order to improve the personal data breach management policies and procedures, and more importantly, to mitigate the risk of any additional breaches in the future.

Other Provisions

A. Our policies and procedures shall be subject to regular revision and review by the Data Protection Officer. The date of the last review and the schedule for the next succeeding review shall be indicated in the documentation of the incident response policy and procedure.
B. The Data Privacy Act and related issuances of the National Privacy Commission, particularly Circular 16-03 shall be deemed incorporated in this Security Policy.

ELECTRONIC MEDICAL RECORDS (EMR) PROVIDER

A. Our EMR Provider, **MedCheck**, is registered with the National Privacy Commission and compliant with the Data Privacy Act and relevant laws and regulations. **MedCheck** implements security measures directed to ensure the availability, integrity, and confidentiality of the personal data being processed, which include: cloud back-up solutions with internationally accredited providers; access control and secure log files; encryption; and policies for data disposal and return of assets.

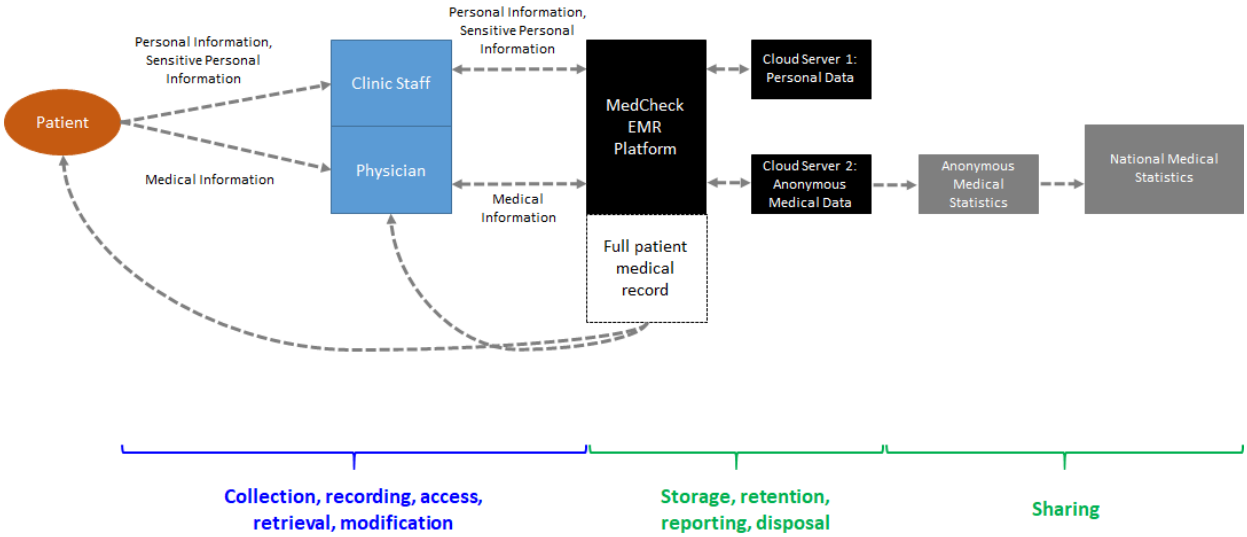
B. **MedCheck** regularly monitors for security breaches and vulnerability scanning of computer networks.

C. **MedCheck** is required to notify our DPO in case of knowledge or reasonable belief that a personal data breach occurred, within 24 hours from knowledge, based on available information.
   a. **MedCheck** shall provide information on the security incident or personal data breach, which shall include: nature, extent and cause, adequacy of safeguards in place, immediate and long-term damage, impact of breach, and its potential harm and negative consequences to affected data subjects.
   b. **MedCheck** shall be asked to contact law enforcement in case criminal activity is suspected.

D. **MedCheck** shall cooperate with our DPO for purposes of complying with breach notification requirements.

E. **MedCheck** may be liable for any personal data breach that occurs when personal data is in its custody, or due to fault or negligence of any of its employees or representatives. **MedCheck** may be liable for any claims from data subjects or any third party, due to the company's failure to comply with terms of the agreement, non-compliance with the law, or when the failure to adequately protect personal data is due to their fault or negligence.

<u>Data Flow Diagram of MedCheck EMR</u>



APPENDIX A: PHYSICIAN'S PRIVACY NOTICE

The clinic respects your right to privacy and knows that your health information is sensitive and confidential. We are committed to protecting you and your personal data.

As a patient of the clinic, we will be making a medical record with your personal information and health information, including the care and treatment you receive. Such information is stored in our Electronic Medical Records software, MedCheck EMR. Both our clinic and MedCheck are registered with the National Privacy Commission and compliant with the Data Privacy Act and other relevant laws and regulations. We uphold your rights as data subjects and have implemented security measures to safeguard your information.

So that we can best meet your medical needs, we may share your medical record and personal information with other health care providers involved in your care. We may also share your personal information for the purposes of collecting payment for the services we provide to you, and to comply with the laws that govern healthcare. We may also use medical information to review our treatment and services and evaluate the performance of our staff in caring for you. Such medical information may also be aggregated with a national, anonymous database, which will be used for medical research. Such research can help improve treatments for patients suffering from the same disease as you. We will not use or disclose your personal information for any other purpose without your permission.

In addition to your healthcare team, our clinic personnel will also have access to your records to contact you for appointments or to provide you with assistance while you are in the clinic. They share the clinic's commitment to protecting your personal data.

Should you require more information, we are happy to assist you. If you believe your privacy rights have been violated, you may raise your concerns with your physician. You may also file a complaint with the National Privacy Commission if we are unable to address your concerns.

APPENDIX B: PATIENT INFORMED CONSENT FORM

Our clinic respects your right to privacy and knows that your health information is sensitive and confidential. We are committed to protecting you and your personal data.

As a patient of the clinic, we will be making a medical record with your personal information and health information, including the care and treatment you receive. Such information is stored in our Electronic Medical Records software, MedCheck EMR. Both our clinic and MedCheck are registered with the National Privacy Commission and compliant with the Data Privacy Act and other relevant laws and regulations. We uphold your rights as data subjects and have implemented security measures to safeguard your information.

Personal Information

Your physician receives and stores the Personal Information and Medical Information that you provide. Personal Information includes information that can identify you, including your first and last name, and contact information. Medical Information pertains to medical conditions and health information provided to and being kept by your physician. While you can choose not to provide Personal Information, some information about you is required in order for the realization of the Purposes below.

Purposes

So that we can best meet your medical needs, we may share your medical record and personal information with other health care providers involved in your care. We may also share your personal information for the purposes of collecting payment for the services we provide to you, and to comply with the laws that govern healthcare. We may also use medical information to review our treatment and services and evaluate the performance of our staff in caring for you. Such medical information may also be aggregated with a national database, which will be used for medical research. Such research can help improve treatments for patients suffering from the same disease as you. We will not use or disclose your personal information for any other purpose without your permission.

Retention

After the completion of the Purposes, your Personal Information and Medical Information may be retained for record purposes for such period that may be permitted by the applicable law, rules and regulations.

Contacting Us

Under applicable laws, you may have the right to object, access, correct, withdraw or remove the Personal Information that is kept. You may also have to right to lodge a complaint with the relevant government agency, with the right to indemnity, for any violation of your rights as a data subject.

For any concerns, please do not hesitate to contact us at the following channels:

Telephone: _____

Email: _____

Office Address: _____

Any request to withdraw your consent given here or to access or correct your Personal Information shall be processed in accordance with applicable laws and regulations.

Amendment

We may amend this Patient Consent Form from time to time and will make available the updated form and secure your consent thereto.

I hereby give my consent to the foregoing:

_____ _____

Patient Name: **Date**

PhilHealth ID:

DOB:

APPENDIX C: DATA BREACH NOTIFICATION TO NPC

<NAME OF ENTITY>
<ADDRESS>
<CONTACT INFORMATION>

<DATE>

<PRIVACY COMMISSIONER>
National Privacy Commission
Pasay City, Metro Manila
Philippines

SUBJECT: <DATA BREACH> of <DATABASE> (NPC Registration No: <NUMBER>), dated <DATE>

Gentlemen:

I write on behalf of <ENTITY>, in relation to the data breach of <DATE>, involving <BRIEF DESCRIPTON OF DATA>. This notification is made pursuant to the mandatory breach notification procedure in Philippine law to the National Privacy Commission.

Responsible Officers. The pertinent details of <ENTITY>, and the responsible persons thereof are as follows:

Head of the Organization:	<NAME>
	<OFFICE ADDRESS>
	<E-MAIL ADDRESS>
	<TELEPHONE>
	<OTHER CONTACT INFO>
Data Protection Officer:	<NAME>
	<OFFICE ADDRESS>
	<E-MAIL ADDRESS>
	<TELEPHONE>
	<OTHER CONTACT INFO>
Process Owner:	<NAME>
	<OFFICE ADDRESS>
	<E-MAIL ADDRESS>
	<TELEPHONE>
	<OTHER CONTACT INFO>

Nature of the Breach:

- <Describe the nature of the personal data breach.>
- <Indicate if breach also affects integrity and/or availability of personal data.>
- <Be as specific as possible. Indicate if details provided are sensitive to the entity, which may cause unwarranted damage to the entity if disclosed to the public.>
- <Provide a chronology that describes how the breach occurred; describe individually the events that led to the loss of control over the personal data.>
- <Further, provide a description of the vulnerability(ies) of the data processing system that allowed the breach.>

- <Include description of safeguards in place that would minimize harm or mitigate impact of personal data breach.>
- <Inform NPC how many individuals or personal records have been affected.>
- <Describe the likely consequences of the personal data breach, including impact on company, data subjects, public, etc.>

Personal Data Possibly Involved:

- <List all sensitive personal information involved, and the form in which they are stored or contained.>
- <List all information involved which may be used to enable identity fraud.>

Measures taken to Address the Breach:

- <Describe in full the measures that were taken or proposed to be taken to address the breach.>
- <Describe effectiveness of measures.>
- <Has the data at risk now been recovered? If not, provide all measures being taken to secure or recover the personal data that were compromised.>
- <Has the organization taken any action to minimize/mitigate the effect on the affected individual? If so, provide all actions being performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident.>
- <Are the affected individuals aware that the incident has occurred? If so, provide all actions being taken to inform the data subjects affected by the incident or any reasons for any delay in the notification.>
- <What steps has your organization taken to prevent a recurrence of the incident?>

Should you require further information on this matter, contact us using the information above. Any information that is indicated as unavailable at this time will be determined and reported within five (5) days, or as soon as possible, as they become available.

Sincerely,

<ENTITY HEAD/DATA PROTECTION OFFICER>

APPENDIX D: DATA BREACH NOTIFICATION TO DATA SUBJECT

<NAME OF ENTITY>
<ADDRESS>
<CONTACT INFORMATION>

<DATA SUBJECT> <DATE>
<ADDRESS>

SUBJECT: <DATA BREACH>, dated <DATE>

Dear <DATA SUBJECT>,

I write on behalf of <ENTITY>, regarding your data in <BRIEF DESCRIPTON OF DATABASE>. We regret to inform you that your data has been exposed in this data breach. To our understanding, your exposure is limited to: <DATA INVOLVED IN THE DATA BREACH.>

Nature of the Breach:

- <Provide a summary of the events that led up to the loss of control over the data. Do not further expose the data subject.>
- <Describe the likely consequences of the personal data breach.>

Measures taken to Address the Breach:

- <Describe in full the measures that were taken or proposed to be taken to address the breach.>
- <Has the data at risk now been recovered? If not, provide all measures being taken to secure or recover the personal data that were compromised.>
- <Has the organization taken any action to minimize/mitigate the effect on the affected individual? If so, provide all actions being performed or proposed to mitigate possible harm or negative consequences.>
- <Are the affected individuals aware that the incident has occurred? If so, provide all actions being taken to inform the data subjects affected by the incident or any reasons for any delay in the notification.>
- <What steps has your organization taken to prevent a recurrence of the incident?>

Assistance to be provided to the Affected Data Subjects:

- <Has the organization taken any steps to provide assistance to the affected individuals? If so, provide all actions being done to assist those who are affected by the incident.>

Do not hesitate to contact our Data Protection Officer for further information:

Data Protection Officer: <NAME>
<OFFICE ADDRESS>
<E-MAIL ADDRESS>
<TELEPHONE>
<OTHER CONTACT INFO>

We will provide more information to you as soon as possible as it becomes available.

Sincerely,

<ENTITY HEAD/DATA PROTECTION OFFICER>

APPENDIX E: ANNUAL SECURITY INCIDENT & DATA BREACH REPORT

SUMMARY

Annual Security Incident and Personal Data Breach Reports

January to December 2017

Total Security Incidents and Personal Data Breaches	<#>
Security Incidents	<#>
Personal Data Breach, Mandatory Notification	<#>
Other Personal Data Breach	<#>

Security Incidents

Attack Vectors

Type	Number
Denial of Service	<#>
Compromised Information (non-personal data)	<#>
Compromised Asset	<#>
Unlawful Activity	<#>
Internal Hacking	<#>
External Hacking	<#>
Malware	<#>
E-Mail	<#>
Policy Violations	<#>
Others	<#>

Personal Data Breaches

	Confidentiality	Integrity	Availability
Mandatory Notification Required	<#>	<#>	<#>
Mandatory Notification Not Required	<#>	<#>	<#>

PREPARED BY: _____ DATE: _____

DESIGNATION: _____