**Sample Template for Data Breach or Imminent Breach Procedures**

 (AGENCY) Data Breach Policy and Procedures

(AGENCY) has implemented the following procedures to follow in the event of a data breach involving personally identifying information (PII) or other confidential information maintained on personal computers, agency networks, or internet programs used by staff and volunteers.

The following staff have key responsibility for implementing and executing the data breach procedures:

* (FIRST RESPONDER) (CONTACT PHONE NUMBERS)
* (SECOND RESPONDER) (CONTACT PHONE NUMBERS)
* (THIRD RESPONDER) (CONTACT PHONE NUMBERS)

In an effort to prevent a breach of data and PII, (AGENCY) has implemented the following measures to prevent the breach of data:

* (TECHNICAL SUPPORT SERVICE PROVIDER)
* (INSTALLED ANTI-VIRUS, INTRUSION NOTIFICATION SOFTWARE)
* (AGENCY PROCEDURES FOR PERSONAL ACCESS AND USE OF AGENCY COMPUTERS)
* (LAW ENFORCEMENT SUPPORT TO LOCATE AND APPREHEND PERPEETRATORS.

(AGENCY) has identified the following items as critical systems and files that will be uploaded to a back-up system on a (DAILY/WEEKLY/MONTHLY) basis:

* (CLIENT DATA FILES)
* (CLIENT CASE FILES)
* (AGENCY FINANCIAL RECORDS)
* (OTHER CRITICAL/CONFIDENTIAL INFORMATION)

In the event of a data breach or imminent breach of PII data, in order to contain the data breach and minimize the extent of the intrusion:

* Disconnect the affected and related systems or networks from Internet access.
* Contact (1st/ 2nd/3rd RESPONDER) to notify them of the data breach or imminent breach of PII data.
* Document date and time the breach occurred, what files the user was accessing at the time of the breach, the breach team member contacted, and actions taken to secure data.
* Contact technical support to detect and remove the malware or other information related to the breach.
* Notify the staff at GCC within 24 hours of the breach occurrence or detection of breach/recognition of imminent breach.
* Review virus/malware/other protective software to review system vulnerabilities and increase the level of protection for the system.
* If possible, reimage the system and restore from backup files.

*Within 24 hours of the breach the Project Director (NAME or DESIGNATED STAFF) must notify the staff at GCC of the data breach, to forward the information to appropriate staff at the federal funding level.*

Following the incident, (AGENCY) staff will review procedures to determine if any actions by the user or the team contributed to the data breach. Staff will be updated on policies to protect against data breaches or imminent breaches of PII data.

A computer technician will review software, updates, and software/data protection programs to improve the security of the data and operating system to prevent further incidents. Information related to the data breach will be documented on the incident log, repairs or modifications implemented will be included on the log and kept in a secure location.

If necessary, the management team will review procedures and make necessary changes to the procedures to improve the security of PII and other secure information.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Agency Name |  | Project ID and Name |  |  |
|  |  |  |  |  |
| Project Director Name |  | Signature |  | Date |
|  |  |  |  |  |
|  |  |  |  |  |
| Authorizing Official |  | Signature |  | Date |
|  |  |  |  |  |