**Hawaii State Department of Education**
***Guidelines for Notification of Security Breaches of Personal Information***

## Purpose

The purpose of these guidelines is to provide a required course of action upon discovery of a security breach of personal information within and from the Hawaii State Department of Education (DOE). These guidelines comply with Hawaii Revised Statutes HRS Chapter 487N, as well as address breaches to personally sensitive information covered by other privacy laws (e.g., Family Educational Rights and Privacy Act (FERPA)).

In accordance with HRS 487N, any government agency shall notify all affected individuals in the event of a security breach involving sensitive personal information. Personal information is defined in HRS 487N. In addition, unauthorized release of confidential information, including those not specifically identified in HRS 487N, should be treated as a security breach and addressed accordingly. The method of notification shall be determined by the DOE in order to facilitate timely notice to those individuals impacted.

The government agency must also submit a report of the security breach to the Legislature in accordance with applicable laws, including but not limited to the Family Educational Rights and Privacy Act (FERPA). See "References, Resources, and Forms" section at the end of this document for further information relating to federal guidance pertaining to student education records.

## Information Security Breaches

Information security breaches include, but are not limited to:

- Computers/Laptops
- Electronic Storage Devices (e.g., USB/flash drives, CDs, DVDs, etc.)
- Email (e.g., sent unsecured to an unauthorized recipient, hacked email inbox, etc.)
- Electronic Documents (e.g., access to unsecured computer by unauthorized individual, failure to destroy files as required, hacked computer, website, server, or database, etc.)
- Paper Documents (e.g., loss, unauthorized duplication or theft of hardcopy, failure to destroy hard copy as required, etc.)

## Personnel Responsibility

In the performance of work for DOE, all employees, volunteers, trainees, and other persons who are under the direct control of DOE, whether or not they are paid by DOE, (hereafter "Personnel") are responsible to report all security breaches that pertain to unauthorized disclosure of personal information from DOE files. The DOE provides a checklist of steps to ensure:

- all instances of a security breach are immediately reported by personnel to their immediate supervisors,

- respective DOE Directors, Complex Area Superintendents, and Assistant Superintendents evaluate each reported security breach incident and determine the appropriate response,

- individuals affected by a security breach are notified immediately following discovery or notification of breach,

- the Data Governance Office (DGO), on behalf of the Superintendent, submits a detailed written report of the security breach incident to the Legislature no later than twenty (20) calendar days from the date of discovery.

**Action Steps** (See Attachment D: *Information Security Breach Checklist)*
Upon discovery of a security breach, the following steps shall be taken:

1. DOE Personnel must inform their respective school principal or section head (hereafter "Supervisor") immediately upon discovery of a known or potential security breach of personal information. It is the responsibility of the Supervisor to immediately evaluate and respond to reported breaches with their respective Complex Area Superintendent, Assistant Superintendent, or Director. Complex Area Superintendents, Assistant Superintendents, and Directors will need to evaluate the scope of the reported breach, as it may lead to breach notification coordination with other DOE offices or government agencies.

2. DOE's Data Governance Office (DGO) should be contacted on the same day of the breach discovery so that they may assist with alerting the breach coordination team and provide guidance and coordination to the office experiencing the breach.

3. The supervisor is to proceed with reporting the security breach of personal information when there is a known unauthorized access, or when there is an immediate probability that an incident will lead to unauthorized access to personal information.
   In HRS 487N, personal information is defined as an individual's first and last name, or first initial and last name, combined with, but not limited to, the following:
   - Social Security Number
   - Driver's License Number or Hawaii State Identification Card Number
   - Account Number, Credit or Debit Card Number, Access Code or Password to an individual's financial account

   Under the Family Educational Rights and Privacy Act (FERPA), "personally identifiable information" ("PII") includes but is not limited to:
   - information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
   - information requested by a person who the school reasonably believes knows the identity of the student to whom the education record relates.

   Personally sensitive information is not limited to the categories listed above. The unauthorized release of any confidential or personally sensitive information should be treated as a security breach. The Supervisor is to report security breach incidents to their respective Complex Area Superintendent, Assistant Superintendent or Director, as well as DGO who will provide guidance and direction on completing the breach evaluation and reporting steps.

4. Police reports are to be filed immediately by the Supervisor for all breach incidents that involve theft of property. In addition, the following office(s) need to be contacted and/or form(s) submitted, depending on the nature of the breach:

a) Theft of a DOE asset is to be reported to the Department of Accounting and General Services (DAGS) – Risk Management Office by completing Form RMP-001 (See References, Resources, and Forms below) and attaching a copy of the police report.
b) Theft of inventory items (i.e., equipment, etc. that are on DOE inventory) must be documented and existing inventory updated by completing the appropriate inventory forms:
    i. Form E-9: Report of Loss or Damage to State Property
    ii. Form FMS-FA 3: Request to Dispose

    Forms and instructions are located at http://fms.k12.hi.us. Questions may be directed to the Office of Fiscal Services (OFS) – Inventory Unit.

If evidence suggesting criminal activity is associated with the security breach, even if no property is involved, it is appropriate to file a police report. DGO should also be notified within 24 hours of any theft event involving information breaches to ensure appropriate assistance and coordination.

5. Upon discovery of a security breach, it should be assumed that personal information will be exposed to further unauthorized access; therefore, all of the following must be done.

    a) Notification must be immediately sent by the Supervisor of the affected organizational unit in coordination with DGO to all individuals whose personal information could be exposed by the breach in security (See Attachment B: *Notification Letter Samples)*. Examples of affected individuals might be owners of personal checks illegally acquired by theft, or individuals included in a database of personal information that has potential to be compromised by someone obtaining username and password without proper authorization. The notification sent to individuals affected by breach of security to personal information must include the following:
        - description of the breach incident in general terms,
        - type of personal information exposed by the breach incident,
        - explanation of actions by DOE to protect the personal information from further unauthorized access,
        - telephone number of office for affected individuals to contact for more information and assistance regarding the breach incident,
        - advice that directs affected individuals to remain vigilant by reviewing account statements and monitoring free credit card reports.

            *Note: By Federal Law, consumers are allowed one (1) free Credit Report per year, from each company/organization offering Credit Report services.*

    b) The scope of the breach must be determined and documented by respective DOE Supervisors. See Attachment E: Information Security Breach - Initial As*sessment and Scope.*

    c) Recommendations to restore security and confidentiality of the affected information system must be documented by the Supervisor and included in the notification to the affected individuals.

d) Notification to affected individuals can only be delayed by an agency of law enforcement that communicates that such notification would impede a criminal investigation or jeopardize national security. Request for delay of notification by law enforcement agencies must be in writing indicating the name of the requesting officer and the requesting agency engaged in the investigation. Upon communication to DOE by the requesting agency that notification to individuals will no longer impede their investigation nor jeopardize national security, notification to affected individuals must commence immediately.

**Acceptable Notification Methods**

Approved methods to notify individuals affected by a breach of security to personal information:

- Written notice mailed to last known address listed in personal record.
- Email notice sent to valid email address in personal record. Such emails may be sent only to those individuals known to have agreed to receive email notifications.
- Telephone notice, provided the contact is made directly with the affected individual.

**Substitute Notification Methods *(under special conditions)***

Substitute notices may be provided if one of the following conditions exist:

- It is demonstrated by DOE that the cost of providing notice to individuals affected by the breach would exceed $100,000.
- The number of individuals affected by the breach will exceed two hundred thousand.
- DOE either does not have sufficient contact information of individuals affected by the breach, or consent for contact via email is not provided for methods listed under the acceptable notification methods above (written, email, or telephone).
- DOE is unable to identify particular affected persons.

<u>Substitute Notification Methods</u>

- Email notice when email address of the individual is available.
- Conspicuous posting of the notice on the DOE website.
- Notice to major statewide media, through the DOE Communications and Community Affairs Office.

6. Additional Notification for Extreme Circumstances

a) If more than one thousand persons at one time are provided notice of a breach of security to personal information, then written notice must also be provided immediately by Supervisor of the affected organizational unit, in coordination with DGO, to the State Department of Commerce & Consumer Affairs, Office of Consumer Protection and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. The notice to Consumer Protection and all consumer reporting agencies must state the timing of the notice sent to individuals affected by the breach of security to personal information, as well as the distribution method, and the content of that notification.

b) Within twenty (20) calendar days after the discovery of a security breach to personal information, DGO, acting on behalf of the Superintendent, shall provide a written report to the legislature, unless a request to delay has been requested by a law enforcement agency because notification would impede a criminal investigation or jeopardize national security. The report will include the following:

- Authorization by the Superintendent, Deputy Superintendent, or Assistant Superintendent acting on behalf of the Superintendent,
- Details of the nature of the breach,
- Number of individuals affected by the breach,
- Copy of the notification sent to individuals affected by the breach,
- Actual number of individuals to whom the notice of breach was sent,
- Indication of whether the notice was delayed by a law enforcement agency,
- Description of procedures implemented to prevent the breach from reoccurring. See Attachment C: *Security Breach Corrective Action Plan Template*.

If the report is delayed due to law enforcement determination that notification may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty (20) days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

A template for the report is provided in Attachment A: *Security Breach – Hawaii State Department of Education, Report to Legislature Template.*

**Found Property**

In the event that DOE property (e.g., computers, laptops, storage devices, documents, etc.) is found, DGO should be notified immediately so that it may be determined if the found property contains confidential or personally sensitive information.

If the found device/property was properly disposed of after the reported theft/loss, and is determined to be in working and useable condition, the office/school should add the item(s) back onto the inventory records. Questions about adding items back onto inventory may be directed to OFS-Inventory Unit.

**Responsibility of the Breach Coordination Team**

Once notified of a breach, DGO will convene a breach coordination team which will consist of representatives from the various offices with data, communication, property, and/or facilities oversight, depending on the nature of the breach. Each representative from the breach coordination team will be responsible for assisting the affected office as it pertains to their area of responsibility (i.e., inventory, equipment, facilities, privacy, etc.) and provide a status to DGO to ensure that all steps are completed in a timely manner.

**References, Resources, and Forms**

| **Hawaii Revised Statutes (HRS)** | |
|---|---|
| *HRS Chapter 487N is in the subdirectory of Volume 11, Chapters 476-490* | http://www.capitol.hawaii.gov/hrscurrent |
| **Form RMP-001** | |
| *The form and instructions, as well as other State forms may be referenced and downloaded from this site* | http://ags.hawaii.gov/aso/rmo/forms-and-instructions/ |
| **DOE Inventory Forms (E-9, FMS-FA 3)** | |
| https://intranet.hawaiipublicschools.org/offices/ofs/accounting/Pages/DefaultFMS.aspx | |
| **Helpful Identity Theft Information** | |
| Federal Deposit Insurance Corporation<br>Federal Trade Commission | http://www.fdic.gov/consumers/consumer/news/cnsprg98<br><br>http://www.ftc.gov/bcp/edu/microsites/idtheft |
| **Credit Card Reporting Companies** | |
| https://www.annualcreditreport.com | |
| **U.S. Department of Education** | |
| Identity Theft | http://www2.ed.gov/about/offices/list/oig/misused/idtheft.html |
| What to Do If a Victim of Identity Theft | http://www2.ed.gov/about/offices/list/oig/misused/victim.html |
| Regulations implementing the Family Educational Rights and Privacy Act, 34 CFR Part 99 (see page FR 78444 for guidance relating to student education records) | http://www.gpo.gov/fdsys/pkg/CFR-2012-title34-vol1/xml/CFR-2012-title34-vol1-part99.xml |

Sample attachments:

- Attachment A: *Security Breach – Information for Report to Legislature*
- Attachment B: *Notification Letter Samples*
- Attachment C: *Security Breach Corrective Action Plan Template*
- Attachment D: *Information Security Breach Checklist*
- Attachment E: *Information Security Breach – Initial Assessment and Scope*

## GLOSSARY OF TERMS

### Breach Guidelines Terms and Definitions

**Authorized Users** – Authorized Users are defined as those users granted access to Personal Information or Data stored (either electronically or in hard copy format) within a physical location or an electronic computer system or transmitted through an electronic communications system.

**Confidential Information** – Any information or data identified as "personal information" (in HRS 487N), "personally identifiable information" (in FERPA), or any combination of information that may put individuals at risk of malicious use of such data (e.g., identity theft, discrimination, etc.).

**Information Security Breach** - An incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential password or login constitutes a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach; provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

**Personal Information -** Personal Data means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social Security Number;
(2) Driver's license number or Hawaii identification card number;
(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account;
(4) Date of birth;
(5) Home/cell/mobile phone and personal mail address.

### Additional Terms and Definitions

The following terms are not referenced in these guidelines but are being provided as additional information.

**Redacted** - Rendering of data or a document so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data.

**IT resources -**means all hardware, software, documentation, programs, information, data, and other devices that are owned or provided by the State. These resources include those that enable remote and local communication such as hubs, switches, routers, and concentrators or access between various platforms and environments such as the mainframe, minicomputers, servers, Local Area Networks ("LANs"), Wide Area Networks ("WANs"), and personal computers.

**Users -**mean all Personnel and students who are authorized to use or access the State's IT resources.

**Data Exchanges** – A "Data Exchange" is defined as a transfer of information between two government entities or between a government entity and non-government entity including vendors,

consultants, financial institutions and other entities doing business with the transferring/receiving agency. The content of the information is usually in a point-time format.

**Data Interfaces** – A "Data Interface" is defined as an active transfer of information between a government entity and any other entity

**Data Retention Policy** – A "Data Retention Policy" contains explicit parameters for the retention of data and information pertinent to government operations and business and includes the Statewide Records Retention Schedule

**Data Disposal Policy –** A "Data Disposal Policy" contains explicit parameters for the proper disposal of data and information containing personal or confidential data or information.

# Security Breach – Information for Report to Legislature

*This report must be completed, and submitted to the Data Governance Office (DGO) upon completion of written notification to affected individuals.*

**Check all boxes that apply.**

Attach the following documents:

1. Initial Assessment and Scope of Information Security Breach.
2. Copy of actual notification sent to affected individuals.
3. Security Breach Action Plan.

**Description of the Information Security Breach**

☐ Initial Assessment and Scope of Information Security Breach attached.

**Method of notification** (check all that apply)

☐ Written notice mailed to last known address listed in personal record.
☐ Email notice sent to valid email address in personal record if individual consented to be notified by email.
☐ Telephone contact made directly with the affected individual.
☐ Email notice when email address of the individual is available (requires justification below).
☐ Conspicuous posting of the notice on the DOE website (requires justification below).
☐ Notice sent to major statewide media via the DOE Communications Office (requires justification below).

**Justification for Use of Substitute Notification Methods** as checked above.

☐ Cost of notifying individuals exceeds $100,000.
☐ The number of affected individuals exceeds 200,000.
☐ Contact information available is insufficient.
☐ Cannot identify all affected persons.

☐ Check box if notification of affected individuals was delayed by a law enforcement agency.

Names: Requesting officer _____Agency_____

Date of request to delay _____ Date of release _____

☐ Copy of the actual notification to affected individuals is attached.

☐ Security Breach Action Plan is attached.

*Point of contact for breach questions from the Legislature:*

_____ _____

Name & Title Date

# Notification Letter Samples

## Sample Notification Letter Regarding Data Breach of Student Information

***To be communicated on DOE Letterhead***

[Recipient Name]
[Recipient Address]

Dear [Recipient first and last name],

We are contacting you to inform you of a recent incident in which you or your child(ren)'s personal information and/or education record may have been compromised. For this reason, we are informing you of this incident and urge you to remain alert to any suspicious activity regarding your child(ren)'s personal information and/or education record by reviewing account statements and monitoring free credit reports. To see more details about the data included in the breached education record, you should submit a request to your child(ren)'s school to review his/her electronic record and cumulative folder.

On [date of breach incident], [description of breach incident in general terms including type of personal information exposed by the breach incident].

In compliance with Hawaii Revised Statutes HRS Chapter 487N and the Family Educational Rights and Privacy Act (FERPA), the DOE has/is taking the following actions to protect personal information from further unauthorized access:

- [list of actions taken]

We urge all potentially affected individuals to take protective measures against identity theft and suggest that you visit the U.S. Department of Education's Office of Inspector General Website, which describes steps students may take if they suspect they are a victim of identity theft, at http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and http://www.ed.gov/about/offices/list/oig/misused/victim.html.

For more information and assistance regarding the incident, please contact [phone number of organizational unit affected by breach].

## Sample Notification Letter for Other Types of Security Breaches

***To be communicated on DOE Letterhead***

[Recipient Name]
[Recipient Address]

Dear [Recipient first and last name],

We are contacting you to inform you of a recent incident where your personal information may have been compromised. For this reason, we are informing you of this incident and urge you to remain alert to any suspicious activity regarding your personal information by reviewing account statements and monitoring free credit reports.

On [date of breach incident], [description of breach incident in general terms including type of personal information exposed by the breach incident].

# Notification Letter Samples

In compliance with Hawaii Revised Statutes HRS Chapter 487N, the DOE has/is taking the following actions to protect your personal information from further unauthorized access:

- [list of actions taken]

We urge all potentially affected individuals to take routine protective measures against identify theft and suggest that you:

- Obtain and carefully review your credit reports. You can order free credit reports from all three credit agencies at http://www.annualcreditreport.com
- Review your bank and credit card statements regularly and look for unusual or suspicious activities.
- Contact appropriate financial institutions immediately if you notice any irregularity in your credit report or any account.
- If your identity or accounts have been compromised, you should take actions such as contacting your financial institution and/or credit card company immediately. Specific recommendations to protect yourself against identity theft and actions you can take if it happens to you are available at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers

For more information and assistance regarding the incident, please contact [phone number of organizational unit affected by breach].

# Security Breach Corrective Action Plan Template

Provide a description of procedures implemented to prevent the breach from reoccurring.

Office Affected _____ Date of the Security Breach _____

Supervisor _____ Point of Contact _____

Brief Description of the Security Breach _____

_____

| **Issue of Concern** | **Action Step** (see next page for examples) | **Tasks Assigned to** (office & individual) | **Date Completed/ Target Date for Completion** | **Funding Required to Complete** | **Funding Source** |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Additional Comments _____

_____

_____

# Security Breach Corrective Action Plan Template (continued)

*The following provides sample actions steps to be taken based on the type of breach occurrence.*

**Unauthorized Entry of Personnel**

1. Install new lock to entrance
2. Provide Awareness Training to personnel

**Network Intrusion**

1. Provide awareness communication
2. Ensure all anti-virus applications running, w/ latest data tables

**Stolen Password**

1. Change passwords on all affected accounts
2. Provide awareness communication
3. Ensure passwords not shared
4. Ensure passwords not displayed open view

**Stolen Document**

1. Provide Awareness training
2. Ensure personnel follow recommended guidelines to protect confidentiality
3. Limit access to affected rooms to authorized personnel

**Lost or Stolen Equipment that Contains Personal Information**

1. Provide Awareness training
2. Ensure personnel follow recommended guidelines to protect confidentiality
3. Ensure use of passwords on devises…

**Hawaii State Department of Education**

***Information Security Breach***

Checklist

*The following checklist is being provided to assist DOE employees in assessing and reporting information security breaches. In the event the responsible person listed is unavailable, the designee or person acting on behalf of the responsible person (e.g., Acting/TA, etc.) should complete the respective action(s).*

**Information security breaches include, but are not limited to, breaches to:**

- Computers/Laptops
- Electronic Storage Devices (e.g., USB/flash drives, CDs, DVDs, etc.)
- Email (e.g., sent unsecured to an unauthorized recipient, hacked email inbox, etc.)
- Electronic Documents (e.g., access to unsecured computer by unauthorized individual, failure to destroy files as required, hacked computer, website, server, or database, etc.)
- Paper Documents (e.g., loss, unauthorized duplication, or theft of hardcopy, failure to destroy hard copy as required, etc.)

| Action to be taken | To be completed | Responsible person/position |
|---|---|---|
| ☐ File a police report if criminal activity is suspected | Immediately upon discovery of breach | Supervisor of the affected organizational unit |
| ☐ Notify supervisor (school principal, section head) | Immediately upon discovery of breach | DOE personnel who discovered breach |
| ☐ Notify additional DOE offices:<br>▪ Complex Area Superintendent, Assistant Superintendent, Director (depending on where breach occurred – school, state office, etc.)<br>▪ Data Governance Office (DGO) | Notification to CAS, AS, Director: immediately upon discovery of breach<br><br>Notification to DGO: same day as breach discovery | Supervisor of the affected organizational unit |
| ☐ Conduct and document initial assessment and scope of breach<br>▪ *Information Security Breach – Initial Assessment and Scope* form | Immediately upon discovery of breach | Supervisor of the affected organizational unit |
| ☐ Complete appropriate forms if theft/loss of property is involved and submit to:<br><u>For Asset (owned) Property: Complete form RMP 001 (attach police report)</u><br>▪ Hawaii Department of Accounting & General Services (DAGS)<br>▪<br><u>Property on DOE inventory: Complete forms E-9 and FMS-FA3</u><br>▪ Hawaii DOE: Office of Fiscal Services (OFS) – Inventory Unit | As required by specified offices/agencies | Supervisor of the affected organizational unit |

**Hawaii State Department of Education**

***Information Security Breach***

Checklist

| Action to be taken | To be completed | Responsible person/position |
|---|---|---|
| ☐ Conduct additional assessment and scope of reported breach | Upon notification by affected organization unit to CAS, AS, or Director | Complex Area Superintendent, Assistant Superintendent, or Director (depending on where breach occurred – school, state office, etc.) |
| ☐ Notify all individuals whose personal information could be exposed by the breach | Immediately upon discovery of breach | Supervisor of the affected organizational unit |
| ☐ Send written notice to the State Department of Commerce and Consumer Affairs (if more than 1,000 persons were provided notice of breach of their personal information) | Immediately upon discovery of breach | Supervisor of the affected organizational unit |
| ☐ Provide written report to the Legislature within twenty (20) days of breach discovery (unless a delay is requested in writing by law enforcement) | Within 20 days of breach discovery<br>**OR**<br>If delay is requested by law enforcement, within 20 days after cleared by law enforcement | Data Governance Office (DGO), acting on behalf of the Superintendent |
| ☐ Direct media inquiries to DOE Communications and Community Affairs Office | As received | Any DOE employee receiving inquiries |

**Hawaii State Department of Education**
***Information Security Breach***
Initial Assessment and Scope

## General Information

Date the breach was discovered: ____/____/20___

Time the breach was discovered: ____:____ AM PM

Location of the breach: _____

Person(s) discovering the breach: _____

## Breach Information

Was criminal activity involved? ☐ Yes ☐ No ☐ Suspected, not confirmed
If yes, was a police report filed? ☐ Yes ☐ No

Was there any theft of property? ☐ Yes ☐ No

What devices/ paperwork were lost, stolen, or breached? _____

_____

If this was an online breach, indicate web address(es): _____

_____

If this was a database breach, indicate database(s): _____

_____

What data might have been breached?
☐ An Individual's Name ☐ Social Security Number
☐ Driver's License Number ☐ Hawaii ID Card Number
☐ Financial Account Information ☐ Health Information
☐ Student Information/Records
☐ Any other specific information that may identify an individual

Can the data be used for fraudulent, malicious, or other purposes? ☐ Yes ☐ No

Is there other information that may be at risk or affected? ☐ Yes ☐ No

**If yes, please describe or list:**

How many individuals and/or records were affected by the breach? _____

Have measures been taken to retrieve data and to block further unauthorized access? ☐ Yes ☐ No

**Describe measures taken to retrieve data and to restore security and confidentiality:**