DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
Mailing: PO Box 661, Trenton, NJ 08625
Location: 33 West State Street 5th Floor, Trenton, NJ 08618

Reporting Damaged/Lost Records Associated with a Cybersecurity Event

In accordance with PL 1953, c. 410/NJSA 47 and PL 2023, c.19, in the aftermath of a cybersecurity event that results in damage and/or loss of public records stored in a computer system(s), once the extent of damage/loss is known and the agency has taken all possible measures to restore the affected records, the agency must submit a Cybersecurity Event Report to the Division of Revenue and Enterprise Services, Records Management Services Unit (RMS) detailing the damage/loss. RMS will present the Report to the State Records Committee (SRC) for disposal authorization.

> Note: Prior to reporting to the SRC, the agency must comply with New State Laws PL 2023, c.19, governing reporting on cyber incidents and breaches. You may access information and report via the New Jersey Cybersecurity and Communications Integration Cell at https://www.cyber.nj.gov/report.

Following are the instructions for reporting damaged/lost records associated with a cybersecurity event to RMS for presentation to the State Records Committee. The instructions include links to the required reporting forms.

Instructions for Reporting: Damaged/Lost Records Associated with a Cybersecurity Event

1. **Download, Complete and Send the Forms** - Listed below, to the Division of Revenue and Enterprise Service, Records Management Services Unit.

    a. Cybersecurity Event Damaged/Lost Records Report <provide url>
    b. Records Inventory for Cybersecurity Event <provide url>
    c. Agency Attestation Regarding Lost or Damaged Public Records Due to a Cybersecurity Event <provide url>

    Mail: PO Box 661, Trenton, NJ 08625
    Attn: RMS Cyber

    or

    Encrypted Email: < >

2. **Respond to any questions posed by RMS** - RMS will review the forms above and reach out to the agency contact with any questions.

3. **After Finalizing the Forms with RMS, Attend the State Records Committee Meeting** - During which the Committee is scheduled to review them. RMS will conduct all required internal reviews with the State Archives and then advise the agency of the date/time of the Committee meeting. RMS will also provide instructions for attendance.

4. **Attend the Committee Meeting and be Prepared to Answer any Questions** - The Committee may take one of several actions:

    a) Send the forms back for further information/clarification, which will require the agency to repeat Steps 1-3;

    b) Formally Approve the premature disposal of the records; or Acknowledge the agency's due diligence in connection with the event and lost/damage records.

    Note: The agency will receive a letter from the Committee in the event of an acknowledgement or approval.

5. **File the SRC-issued Acknowledgement or Approval** – Permanent retention.

6. **Provide Future Requestors Seeking Access to the Involved Records with an Attestation** – Detailing their loss/damage (see example template). <provide url>

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
Mailing: PO Box 661, Trenton, NJ 08625
Location: 33 West State Street 5th Floor, Trenton, NJ 08618

SENSITIVE/CONFIDENTIAL

Damaged/Lost Records Report Due to Cybersecurity Event
<Date>

Agency Name: ____

Address: ____

Phone: ____

Email: ____

Contact Person: ____

Date the Cyber Attack Occurred: ____

Date the Cyber Attack was Discovered: _____________________________________

Complete the following.

1. List the records affected by the event.

2. Describe the circumstances in which the event occurred and how it was discovered?

3. Were IT and cyber security professionals contacted for help and what measures were taken to identify and block the event?

4. Were any records affected by this event recoverable? Detail the recovery attempts made.

5. If records were not recoverable, which official(s) made the determination? (Provide name(s) and title(s))

6. Are there other copies of the records or can they be reconstructed (e.g. payroll records may be recovered from a payroll service provider)?

7. Are recovered records, if any, kept in the storage platform where the event occurred? If yes, how are these records now being protected from future attacks?

8. Did the agency make the required notification as per State Law PL 1953, c. 410/NJSA 47 and PL 2023, c.19?

□ **Yes**

□ **No**

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
PO Box 661, Trenton, NJ 08625

Records Inventory
Public Records Affected by Cybersecurity Event
<Date>

Agency Name: ____

Agency Retention Schedule: ____

Retention Schedule Number: ____

Record Series Number: ____

Record Series Name: ____

Retention Time: ____

Inclusive Years: ____

Backup Copies Available? ____

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
PO Box 661, Trenton, NJ 08625

Public Records
Agency Attestation Regarding Lost or Damaged Public Records
Due to a Cybersecurity Event

TO: State Records Committee

FROM: <Agency>

DATE: <Date>

SUBJECT: Cyberattack of Agency-owned Public Records

I hereby attest that due to a cybersecurity event that occurred on or around <Date>, the records listed below were lost and/or damaged. The above-referenced made diligent efforts to recover all lost/damaged records.

____
Signature and Title

____
Date

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
PO Box 661, Trenton, NJ 08625

New Jersey State Records Committee Acknowledgement
Public Records Lost/Damaged Due to a Cybersecurity Event
<Date>

TO: ____

FROM: DIVISION OF REVENUE AND ENTERPRISE SERVICES (DORES),
RECORDS MANAGEMENT SERVICES (RMS)

DATE: ______________________________

SUBJECT: New Jersey State Records Committee (SRC)-Acknowledgement of
Public Records Lost or Damaged Due to a Cybersecurity Event

The New Jersey State Records Committee acknowledges the cybersecurity event and loss and/or damage of records from <Agency> as shown in the attached attestation, and recognizes the due diligence the Agency has shown in coming before the Committee. This Acknowledgement is therefore formally entered into the Minutes of the New Jersey State Records Committee. Representatives from <Agency> and Records Management Services Staff presented the acknowledgement to the Committee on <Date>.

Signature: ____ Date: ______________________________

Secretary, State Records Committee

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
PO Box 661, Trenton, NJ 08625

Public Records
Attestation to Records Requestors

TO: Records Requestor

FROM: <Agency Date>

DATE: <Date>

SUBJECT: Cyberattack of Agency-owned Public Records

I hereby attest that the records listed below were affected by a cybersecurity event that occurred on or around <Date.>. <Agency> made diligent efforts to obtain, retrieve and salvage these records. As a result of this, <Agency>:

□ Cannot provide the requested records

□ Can provide portions of the records, but due to the cybersecurity event, cannot verify the completeness or accuracy of the records

____
Signature and Title

____
Date