



# STATE OF CONNECTICUT

## INSURANCE DEPARTMENT

### **CYBERSECURITY REPORTING FORM**

#### **CONTACT INFORMATION**

Name:

Address Line 1:

Address Line 2:

City:

State/Area:

Postal Code:

Telephone:

Fax:

E-mail Address:

#### **EVENT DATES**

Identify the time period that the security event involved.

Identify the date that the security incident was discovered.

#### **CIRCUMSTANCES**

How was the Cybersecurity Event discovered?

What type of event occurred, phishing or malware? Is this a ransomware incident?

How was the information exposed, lost, stolen or accessed? Include the identity of the source of the Cybersecurity Event, if known.

Does this incident involve an internal employee? Were they working remotely? What type of acceptable use policy is in place? Please provide date of origination.

[portal.ct.gov/cid](http://portal.ct.gov/cid)

P.O. Box 816 Hartford, CT 06142-0816  
An Equal Opportunity Employer

**THIRD-PARTY INVOLVEMENT**

Did the Cybersecurity Event involve a third-party service provider?                      Yes                      No

If yes, please identify the name of the third-party service provider and the nature of the work performed on behalf of the licensed entity.

Does the incident response plan sufficiently address steps to take when a Cybersecurity Event occurs at a Third-Party Service Provider where data provided by Licensee is potentially at risk?

**INFORMATION INVOLVED**

Did the cybersecurity event involve the licensed entity’s systems?

Does the company use algorithms or any other type of artificial intelligence (AI)?

Describe the specific types of information acquired. For example, types of medical information, types of financial information, or types of information allowing the identification of the consumer.

Was the electronic information encrypted?                      Yes                      No

If no, please provide an explanation.

**NUMBER OF INDIVIDUALS/ENTITIES AFFECTED**

Please identify the number of individuals affected in Connecticut and on a nationwide basis.

**REMEDIATION**

What actions are being taken to recover lost, stolen or improperly accessed information?

What steps were undertaken to remediate the situation once the Cybersecurity Event was detected?

Is there a ransomware remediation plan currently in place? How often is it tested?

Has any lost, stolen or breached information been recovered?

**NOTIFICATION REQUIREMENTS**

Is there a reasonable likelihood that the information obtained has been or will be misused?

**REPORTING REQUIREMENTS**

Has a police report been filed?

Has any regulatory, governmental, or other law enforcement agency been notified?

**CYBERSECURITY CONTACT DESIGNEE**

Contact Information of Individual Familiar with Cybersecurity Event and Authorized to Act on Behalf of the Licensee

Prefix

First Name

Middle Name

Last Name

Title

**CONTACT METHODS**

Home Phone:

Business Phone:

Mobile Phone:

Fax:

E-mail

Address

City:

State/Area:

Postal Code:

**ATTACHMENTS ITEMS:** (Please submit via e-mail)

- A copy of the licensee’s privacy policy
- A copy of its security incident response policy
- The notice to be submitted to the affected party/parties
- Electronic device acceptable use policy
- Disaster recovery plan

**CERTIFY & SIGN**

Please note that the individual submitting this information certifies that the information provided above is true and accurate to the best of his/her knowledge.

Please note that the date remitted to the department will be the date first reported by the entity.

Complete this form and submit via e-mail to [cid.mc@ct.gov](mailto:cid.mc@ct.gov) include all attachments items require.

Signature:

Date: