

## DATA BREACH POLICY FOR THE OFFICE OF POLICY & MANAGEMENT

### Revision History

Version	Date of Revision	Author	Description of Changes
1.0	September 19, 2022	IT Policy Development Team	Initial version

**Purpose** – The purpose of this internal policy is to define the process for reporting a Confidential Information Breach, for the Office of Policy & Management’s (“OPM”) employees, fellows, interns, consultants, and partners, and to identify roles and responsibilities for responding to a report of a breach, and to establish feedback mechanisms to enable investigation and remediation. This policy applies to all OPM employees, fellows, interns, consultants, and partners whose duties involve the handling of private, confidential, sensitive, protected, or restricted data (i.e., electronic or paper) as identified by OPM in the inventory of Confidential or Restricted Information (see Attachment A), updated annually.

OPM’s intentions for publishing this Data Breach Policy are to raise awareness, focus significant attention on data security and privacy, and communicate clearly the steps to be taken when an incident occurs. OPM is committed to protecting its role as a data steward and, as such, requires all employees, fellows, interns, consultants, and partners to become familiar with the policy and take the necessary steps to comply.

**Scope** – This policy applies to any OPM individuals, fellows, interns, consultants, and partners who collect, access, or possess Confidential or Restricted Information. Any agreements with vendors, partners, consultants, intermediaries shall contain language clearly pointing to this policy.

**Process for Reporting an Incident** – This policy mandates that any individual who suspects that a theft, loss, breach, or exposure of Confidential or Restricted Information has occurred must immediately (i.e., 24 hours or less) contact [OPM.Incidents@ct.gov](mailto:OPM.Incidents@ct.gov) and provide a detailed description of what occurred, data believed to have been compromised, and contact information for follow-up. This information will be used by the OPM Incident Response Team to begin its investigation and notify the appropriate agencies/authorities based on the scope of the data in question and severity of the breach. The OPM Incident Response Team, depending on the nature of the data breach, shall reach out to the Department of Administrative Services (“DAS”) Bureau of Information Technology Services (“BITS”) Helpdesk to notify the DAS BITS Security Team and any other parties to assist in the investigation, terminate unauthorized access, and notify appropriate state and federal partners, if necessary. Attachment B provides a process flowchart individuals can use to comply with this policy and Attachment C provides a list of contacts that need to be notified if an event occurs.

### Roles and Responsibilities

- **OPM Employees, interns, fellows, consultants and partners** – Review policy and subsequent revision when published. Participate in an orientation session and ask questions. Protect data you have access to, whether in paper or electronic form. Immediately report an incident by providing as much information and as quickly as possible. Be available to provide additional information and answer questions as incidents are escalated for review and investigation.
- **OPM Incident Response Leader** – Actively monitor [OPM.Incidents@ct.gov](mailto:OPM.Incidents@ct.gov) and review incidents as quickly as possible. Perform initial review to confirm incident and notify the OPM Incident Response Team, which will automatically receive a copy of the OPM.Incident@ct.gov electronic communication detailing the incident once submitted. If necessary, escalate and engage appropriate agencies/partners to identify, contain, and terminate unauthorized access. Prepare a post-incident activity report summarizing the incident from start to conclusion.
- **OPM Incident Response Team** – Support the OPM Incident Response Leader in carrying out the procedures to respond to the data breach incident. Support efforts to raise awareness and lead by example. Engage

OPM staff to improve organizational hygiene and security posture. Provide feedback for inclusion in the Post-Incident Activity report.

- **State Information Security Team** – State Chief Information Security Officer (“CISO”) and State Chief Information Officer (“CIO”) who will reach out to their respective staff based on the nature, scope, and severity of breach.

**Monitoring Compliance** – review regularly with a minimum frequency of once per year.

- 1) All OPM staff shall review this policy annually and division heads shall document staffs’ completion of such review.
- 2) OPM Agency Data Officer and Chief Data Officer will review with agency data stewards all data in the Confidential and Restricted Information list to maintain awareness and answer any new questions.
- 3) OPM will periodically coordinate an exercise or simulation for a breach to gauge response and address any gaps.

### Definitions

“Confidential information” means an individual's name, date of birth, mother's maiden name, motor vehicle operator's license number, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation, personally identifiable information subject to 34 CFR 99, as amended from time to time and protected health information, as defined in [45 CFR 160.103](#), as amended from time to time. In addition, “confidential information” includes any information that a state contracting agency identifies as confidential to the contractor. “Confidential information” does not include information that may be lawfully obtained from publicly available sources or from federal, state, or local government records that are lawfully made available to the general public.

“Confidential information breach” means an instance where an unauthorized person or entity accesses confidential information that is subject to or otherwise used in conjunction with any part of a written agreement with a state contracting agency in any manner, including, but not limited to, the following occurrences: (A) Any confidential information that is not encrypted or secured by any other method or technology that renders the personal information unreadable or unusable is misplaced, lost, stolen or subject to unauthorized access; (B) one or more third parties have accessed, or taken control or possession of, without prior written authorization from the state, (i) any confidential information that is not encrypted or protected, or (ii) any encrypted or protected confidential information together with the confidential process or key that is capable of compromising the integrity of the confidential information; or (C) there is a substantial risk of identity theft or fraud of the client of the state contracting agency, the contractor, the state contracting agency or the state.


### Incident Types


“Denial of Service” means an incident by which authorized access to systems or data is prevented or impaired. Usually a denial of service (“DoS”) incident is a security event if the DoS is due to malicious intent. Not all events that prevent or hinder authorized access to systems or data are security incidents. The mechanical, electrical, or administrative failure of a system or access mechanism may not be a security incident.

“Unauthorized Access” means an incident where unauthorized access is attempted or gained to systems or data. This access can be logical or physical in nature. Unauthorized access is any access for which permission has not been granted. Such permissions would include connect, authenticate, read, write, create, delete, modify, copy, scan, etc. This unauthorized access can be by an individual or another system.

## DATA BREACH POLICY FOR THE OFFICE OF POLICY & MANAGEMENT

**Inappropriate Usage:** An incident by which acceptable use policies are violated. Acceptable use policies may include what types of data may be accessed or transmitted, how information may be accessed or transmitted, and where information may be received from or transmitted to.

 9-20-22  
\_\_\_\_\_  
Jeffrey R. Beckham                      Date  
Secretary

 20 SEP 22  
\_\_\_\_\_  
Paul E. Potamianos                      Date  
Deputy Secretary



# DATA BREACH POLICY FOR THE OFFICE OF POLICY & MANAGEMENT

## Attachment A – List of Confidential and Restricted Information as of 2022

Description of Information	Authority
<p>EMPLOYEE INFORMATION</p> <ul style="list-style-type: none"> <li>• Social security numbers.</li> <li>• Dates of birth.</li> <li>• Employee numbers.</li> <li>• Home addresses and telephone numbers of staff who have PO Boxes and unlisted telephone numbers.</li> <li>• Personal cell phone numbers.</li> <li>• Personal e-mail addresses.</li> <li>• Personally identifiable data through Core-CT.</li> <li>• Personally identifiable data through CATER.</li> <li>• Social security numbers in pre-Core-CT data.</li> <li>• Birth certificates, social security numbers and marriage licenses of dependent(s).</li> <li>• Birth certificates, social security numbers and address of beneficiary(s).</li> <li>• Health and group life insurance applications as these applications contain personally identifiable information.</li> <li>• Drivers' license numbers, motor vehicle license plates and identification information.</li> <li>• Motor vehicle insurance information.</li> </ul>	<p>OPM protects various types of employee information in accordance with the following:</p> <ul style="list-style-type: none"> <li>• C.G.S. Sec. 1-210(b)(2)</li> <li>• C.G.S. Sec. 7-51</li> <li>• Privacy Act of 1974, as amended (5 U.S.C. 552a)</li> </ul>
<p>VENDOR AND GRANTEE INFORMATION</p> <ul style="list-style-type: none"> <li>• Social security numbers, federal employer identification numbers, and/or state tax identification numbers. Note: OPM will share federal employer identification numbers with other state agencies.</li> <li>• Personally identifiable data through Core-CT.</li> <li>• Birth dates, telephone numbers, e-mail addresses and medical information included on grantee applications including but not limited to Renters, Homeowners, Totally Disabled, and Veterans.</li> </ul>	<p>OPM protects various types of vendor and grantee information in accordance with the following:</p> <ul style="list-style-type: none"> <li>• C.G.S. Sec. 1-210(b)(2)</li> <li>• Privacy Act of 1974, as amended (5 U.S.C. 552a)</li> </ul>
<p>OTHER PERSONALLY IDENTIFIABLE INFORMATION</p> <ul style="list-style-type: none"> <li>• Social security numbers on old job applications and other information on paperwork for prospective employees and interns including, but not limited to, name, mailing address, email address, phone number, and transcripts.</li> <li>• Social security numbers and dates of birth of CT Partnership policy holders.</li> </ul>	<ul style="list-style-type: none"> <li>• C.G.S. Sec. 1-210(b)(2), Privacy Act of 1974, as amended (5 U.S.C. 552a), and March 1990 Personnel Director v. FOI Commission ruling.</li> <li>• C.G.S. Sec. 1-210(b)(2), Privacy Act of 1974, as amended (5 U.S.C. 552a) and FOI Advisory Opinion #78 dated February 23, 1990</li> </ul>

# DATA BREACH POLICY FOR THE OFFICE OF POLICY & MANAGEMENT

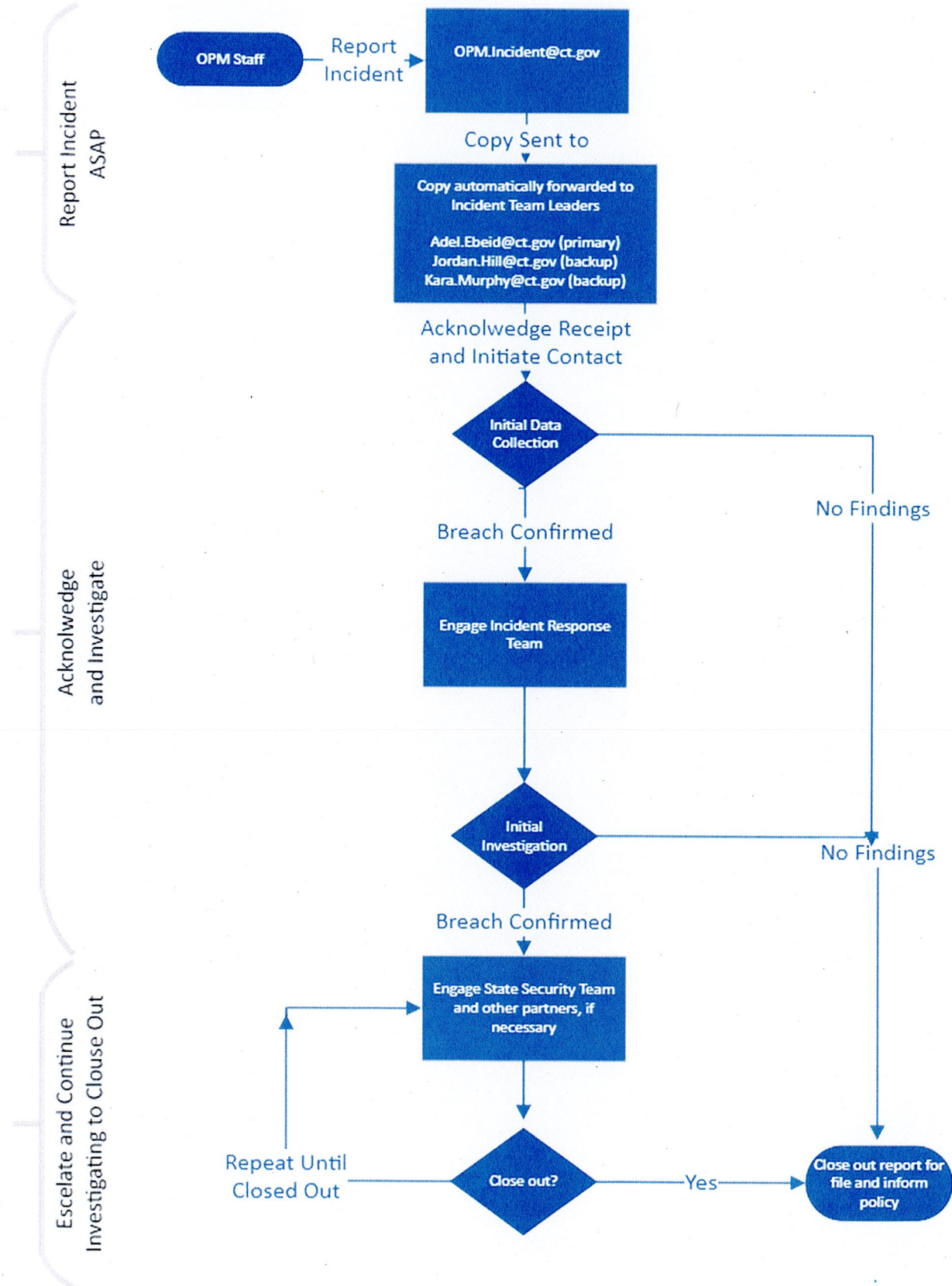
<ul style="list-style-type: none"> <li>• Social security numbers of insurance agents.</li> <li>• Social security numbers, home address, and dates of birth for inmates and individuals involved in the criminal justice system.</li> <li>• Social security numbers and federal employer identification numbers of revaluation companies and their certified employees.</li> <li>• Student ID Numbers provided by CT State colleges and universities as part of the United We Stand license plate grant program.</li> </ul>	<ul style="list-style-type: none"> <li>• C.G.S. Sec. 1-210(b)(2), Privacy Act of 1974, as amended (5 U.S.C. 552a) and FOI Advisory Opinion #78 dated February 23, 1990</li> <li>• C.G.S. Sec. 1-210(b)(2) and Privacy Act of 1974, as amended (5 U.S.C. 552a); C.G.S. Secs. 4-68m(e)(2) and 4-68m(e)(3)</li> <li>• C.G.S. Sec. 1-210</li> <li>• C.G.S. Sec. 1-210(b)(2) and Privacy Act of 1974, as amended (5 U.S.C. 552a)</li> <li>• C.G.S. Sec. 1-210(b)(2) and Privacy Act of 1974, as amended (5 U.S.C. 552a)</li> </ul>
<p><b>BUDGET INFORMATION</b></p> <ul style="list-style-type: none"> <li>• Budget-related matters that are considered confidential as the Governor's Budget proposals are developed.</li> <li>• Legislative-related matters that are considered confidential as the Governor's Budget and legislative proposals are developed.</li> <li>• Budget-related matters that are considered confidential as the OPM works with the legislature to develop and negotiate a budget.</li> <li>• Legislative-related matters that are considered confidential as OPM works with the legislature to develop and negotiate a budget and related legislation.</li> </ul>	<ul style="list-style-type: none"> <li>• C.G.S. Secs. 1-210(b)(1) and 1-210(e)</li> <li>• C.G.S. Secs. 1-210(b)(1) and 1-210(e)</li> <li>• C.G.S. Secs. 1-210(b)(1) and 1-210(e)</li> <li>• C.G.S. Secs. 1-210(b)(1) and 1-210(e)</li> </ul>
<p><b>LABOR RELATIONS INFORMATION</b></p> <ul style="list-style-type: none"> <li>• Contract negotiations.</li> <li>• Pending matters relating to grievances and arbitration.</li> </ul>	<ul style="list-style-type: none"> <li>• C.G.S. Secs. 1-210(b)(9) and 1-210(b)(10)</li> <li>• C.G.S. Secs. 1-210(b)(4) and 1-210(b)(10)</li> </ul>
<p><b>LEGAL INFORMATION</b></p>	



<ul style="list-style-type: none"> <li>Records, reports, notes, statements of strategy, or statements of negotiations pertaining to pending matters including but not limited to bids, claims, litigation, settlement agreements, contracts, or collective bargaining.</li> <li>Attorney work product and/or confidential attorney communications and/or privileged communications.</li> </ul>	<ul style="list-style-type: none"> <li>C.G.S. Secs. 1-210(b)(4) and 1-210(b)(10)</li> <li>C.G.S. Secs. 1-210(b)(10) and 52-146r</li> </ul>
<p>MISCELLANEOUS</p> <ul style="list-style-type: none"> <li>Education Records</li> <li>Numeric grades of individuals taking revaluations examinations.</li> <li>State Purchasing Card account numbers, cards and related documents.</li> <li>Tobacco Settlement Fund report from Pricewaterhouse Coopers</li> <li>Water Plan Information</li> </ul>	<ul style="list-style-type: none"> <li>C.G.S. Secs. 1-210(b)(17), 1-210(b)(11) and <a href="#">Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)</a></li> <li>C.G.S. Secs. 1-210(b)(2) and 1-210(b)(6)</li> <li>"State of Connecticut Credit Card Use Policy" found at: <a href="http://das.ct.gov/images/1090/CC_Policy_12_11_14.pdf">http://das.ct.gov/images/1090/CC_Policy_12_11_14.pdf</a></li> <li>C.G.S. Sec. 1-210(b)(5); see 9-8-16 Tassinari email, the reports contain specific private industry information</li> <li>C.G.S. Sec. 1-210(b)(19) (ix)</li> </ul>
<p>REQUESTS FOR PROPOSALS (RFP)/REQUESTS FOR QUALIFICATIONS (RFQ) INFORMATION</p> <ul style="list-style-type: none"> <li>Responses to requests for proposals until such contract is executed or negotiations for the award of such contract have ended, whichever occurs earlier</li> <li>As part of RFP/RFQ submissions, confidential financial and/or trademark information that is exempt from the Freedom of Information Act.</li> <li>Preliminary financial information and cost estimates which could impact public bidding and selection processes.</li> </ul>	<ul style="list-style-type: none"> <li>C.G.S. Sec. 1-210(b)(24)</li> <li>C.G.S. Secs. 1-210(b)(5)(A) and 1-210(b)(5)(B)</li> </ul>

	<ul style="list-style-type: none"> <li>C.G.S. Sec. 1-210(b)(24)</li> </ul>
<p>CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)</p> <ul style="list-style-type: none"> <li>Background check information, including but not limited to, fingerprint cards and results.</li> <li>CJIS security policies for CISS implementation.</li> <li>Any and all information related to CJIS systems: OBTS, CIDRIS, and CISS.</li> </ul>	<p>CJIS protect information in accordance with the following:</p> <ul style="list-style-type: none"> <li>Federal Information Security Management Act of 2002</li> </ul>
<p>CRUMBLING FOUNDATIONS DATA</p> <ul style="list-style-type: none"> <li>Crumbling Foundations Testing Reimbursement Program Database: Database funded by the Department of Housing (DOH) and administered by the Capitol Region Council of Governments (CRCOG). Available online with authorized login and password at <a href="https://www.foundationtesting.org/">https://www.foundationtesting.org/</a>. <ul style="list-style-type: none"> <li>Fields include applicant name and contact information, home address, home characteristics, test results, application status, and reimbursement information.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>C.G.S. Sec. 32-41qq</li> </ul>
<p>BROADBAND INTERNET ACCESS SERVICE PROVIDER DATA</p> <ul style="list-style-type: none"> <li>Address-level data for service availability from internet service providers</li> <li>Internet service subscription data including both counts at the census tract-level at each speed tier and address-level subscription data</li> </ul>	<ul style="list-style-type: none"> <li>P.A. 21-159</li> </ul>

Attachment B – Data Breach Incident Reporting Flowchart





Attachment C – List of Contacts

- To Report a Data Breach Incident [OPM.Incidents@ct.gov](mailto:OPM.Incidents@ct.gov)
- Incident Team Leader
  - **Primary Contact**  
Adel Ebeid, Sr IT Policy Advisor  
[Adel.Ebeid@ct.gov](mailto:Adel.Ebeid@ct.gov)  
Office 860.418.6432  
Mobile 860.944.8326
  - **Secondary Contact**  
Jordan Hill, IT Analyst  
[Jordan.Hill@ct.gov](mailto:Jordan.Hill@ct.gov)  
Office 860.418.6389  
Mobile 860.904.0218
  - **Tertiary Contact**  
Kara Murphy, Staff Attorney  
[Kara.Murphy@ct.gov](mailto:Kara.Murphy@ct.gov)  
Office 860.418.6233  
Mobile 860.593.8543
- Incident Response Team
  - Sr IT Policy Advisor
  - OPM IT Manager
  - Chief Data Officer
  - Agency Data Officer
  - OPM General Counsel
  - OPM Communications Leader
- State Security Team
  - CT Chief Information Officer
  - CT Chief Information Security Officer