BRYT SECURITY INCIDENT RESPONSE POLICY

PURPOSE

This policy is designed to improve the response time to Bryt Software (hereinafter referred to as Bryt) security incidents, improve incident reporting and related communications, mitigate any damages caused by incidents, and improve overall data security systems.

POLICY

Bryt will maintain guidelines and procedures to provide the basis for appropriate responses to incidents that threaten the security, confidentiality, integrity, and/or availability of Bryt information assets, information systems, and/or networks that deliver the information as well as client information. Bryt data security guidelines and procedures will be reviewed periodically and updated as necessary.

Guidelines and Definitions

This policy applies to Bryt and all systems and services for which it is responsible.
An incident is any event that threatens the security, confidentiality, integrity, or availability of Bryt information assets, information systems, and/or the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an incident. Incidents may include:

- Unauthorized entry
- Security breach
- Unauthorized scan or probe
- Denial of service
- Malicious code or virus
- Other violations of the Bryt Acceptable Use Policy
- Networking system failure (widespread)
- Application or database failure (widespread)
- Others as defined by critical incident response teams

Incidents such as those listed above vary in their impact on Bryt and in the degree of risk and vulnerability they pose.

A “security breach” is defined as the unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information. A “security breach” does not include good faith, but unauthorized acquisition or access of personal information by an employee of Bryt for legitimate business purposes.

For the purpose of this policy, and in accordance with State law, personal information 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 or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:

- social security number;
- full name

- email address
- home address
- financial account number, if circumstances exist in which the number could be used without additional identifying information;
- access codes or passwords;
- account passwords or personal identification numbers or other access codes for a Bryt user account.

Personal information does not mean publicly available information that is lawfully made available to the general public from federal, state, or local records.

Critical Incidents are defined as "high impact and high risk"; these include the known or suspected compromise of personal information or institutional proprietary information to entities outside Bryt or to entities inside Bryt for non-legitimate purposes. Critical incidents require the development and implementation of a formal incident response action plan by the critical incident response team.

Non-Critical Incidents are defined as "low or medium risk"; these may include good faith but unauthorized acquisition or access of personal information by an employee for a legitimate business purpose, viruses, worms, compromised machines, or other non-critical or minor issues. Non-critical incidents do not require a formal incident response action plan but must have an appropriate response, as determined by the President/designee and Chief Information Officer (CIO).

Critical Incident Response Teams will be established at Bryt; overall membership will include:

- Executive leadership
- legal counsel
- IT leadership (network, software development, database, and security)
- communications personnel

Participation by individual members may vary by incident as appropriate. Members of critical incident response teams are expected to respond immediately and fully when called upon. Responding to a critical incident, in general, takes precedence over all other work. If a member is unavailable at the time the team is assembled, a substitute member may be named by the chair or executive leadership.

An incident is declared to be critical in one of the following ways:

- the President or designee, declares an incident to be critical.
- the Security Officer, CIO, or designee, in consultation with the President or designee, declares an incident to be critical.

Procedures

1. Upon discovery or suspicion of an incident, Bryt employees shall notify IT Services in a prompt and effective manner through a phone call directly to the Security Officer, CIO/

designee, or the President/designee.

2. Within four business hours of receipt of notification or suspicion of an incident, the CIO/ designee or the Security Officer will; remove the risk, if possible; and begin an investigation of the incident, including notification to the critical incident response team. The CIO or the Security Officer will keep a log of all activity related to the investigation.

3. Within one business day of receipt of notification, the critical incident response team, in consultation with the President/ designee will determine whether the incident is critical or non-critical.

4. *If the incident is determined to be non-critical*, public notice of the incident is not required, but an appropriate response will be determined by the President/ designee, the Security Officer, and CIO; the response may include a change in policy or practice, required training, targeted communications or further inquiry. The CIO or the Security Officer will submit to the President a brief description of the incident and the rationale for determining it to be non-critical. The procedures for a non-critical incident end at this step.

5. *If the incident is determined to be critical*, the critical incident response team will follow all remaining procedures. The team will review the incident, create an overall action plan and formulate an appropriate system response; this response may include but is not limited to:
   - assuming control of and containing the incident; involving appropriate personnel, as conditions require;
   - conducting a thorough investigation of the incident, including establishing controls for the proper collection and handling of evidence, and keeping a log of all communications and actions related to the incident;
   - determining whether or not to involve outside personnel, such as law enforcement or computer forensic experts;
   - drafting statements and materials for public notice as required by State law;
   - executing a remediation plan, possibly including repairing/ rebuilding any damaged systems and considering any additional remedies for affected constituents;
   - recommending any change in policy or practice, required training, targeted communications, or further inquiry;
   - monitoring and revising the action plan as needed in the period directly following the incident;
   - discussing, reviewing, and documenting all actions and results, and particularly any lessons learned from the security breach.

6. Within one business day of receipt of notification, unless authorized for extended review by the President or designee, the critical incident response team will confirm with executive leadership at Bryt a preliminary course of action.

7. In accordance with applicable laws, the critical incident response team will notify affected constituents without unreasonable delay, generally within two business days of receipt of notification. Notice will include a description of the following:

- the incident in general terms;
- the type of personal information that was subject to the "security breach" or acquisition;
- the general acts of Bryt to protect the personal information from further unauthorized access or acquisition;
- a toll-free number that constituents may call for further information and assistance;

Notice may be provided by one of the following methods:

- telephonic notice directly with the constituent and not through a prerecorded message, or
- electronic notice if phone information is not available; electronic notice cannot request personal information and must conspicuously warn constituents not to provide personal information in response to electronic communications regarding security breaches.

8. The critical incident response team will conduct a post-incident critique and submit a summary report to the President including:

- a description of the incident
- a summary of lessons learned
- any suggested changes to existing policies or procedures
- any recommendations to protect against future incidents

9. Any disciplinary action considered in association with a critical incident shall follow procedures set forth in the Bryt personnel handbook.

NOTES:

- Reporting Requirements:
  - General Data Protection Regulation (GDPR) which went into effect on 05/25/2018 requires you to report any breaches to the data subject or the supervisory authority within 72 hours.
  - Look into SOC 2 & ISO/IEC 27001 for more reporting requirements
- Information accessible in Contacts
  - Full name (First, middle, last)
  - Address (Street, City, State, ZIP)
  - Email address
  - Phone number
  - Last 4 of SSN

Table 3-2. Functional Impact Categories

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Table 3-3 provides examples of possible information impact categories that describe the extent of information compromise that occurred during the incident. In this table, with the exception of the 'None' value, the categories are not mutually exclusive and the organization could choose more than one.

Table 3-3. Information Impact Categories

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Table 3-4 shows examples of recoverability effort categories that reflect the level of and type of resources required to recover from the incident.

Table 3-4. Recoverability Effort Categories

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation