2. Policy Management Policy

Ceresti implements policies and procedures to maintain compliance and integrity of data. The Security Officer and Privacy Officer are responsible for maintaining policies and procedures and assuring all Ceresti employees, business associates, customers, and partners are adherent to all applicable policies. Previous versions of policies are retained to assure ease of finding policies at specific historic dates in time.

2.1 Applicable Standards

2.1.1 Applicable Standards from the HITRUST Common Security Framework

- 12.c - Developing and Implementing Continuity Plans Including Information Security

2.1.2 Applicable Standards from the HIPAA Security Rule

- 164.316(a) - Policies and Procedures
- 164.316(b)(1)(i) - Documentation

2.2 Maintenance of Policies

1. All policies are stored and updated to maintain Ceresti's compliance with HIPAA, HITRUST, NIST, and other relevant standards. Updates and version control are done similarly to source code control.
2. Policy update requests can be made by any employee at any time. Furthermore, all policies are reviewed annually by both the Security and Privacy Officer to assure they are accurate and up-to-date.
3. Ceresti employees may request changes to policies using the following process:
    1. The Ceresti employee initiates a policy change request by creating an Issue in the Ceresti Quality Management System.
    2. The Security Officer or the Privacy Officer is assigned to review the policy change request.
    3. Once the review is completed, the Security Officer or Privacy Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.
    4. If the review is approved, the Security Officer or Privacy Officer adds any pertinent notes required.
    5. If the policy change requires technical modifications to production systems, those changes are carried out by authorized personnel using Ceresti's change

management process (§8.4).

4. All policies are made accessible to all Ceresti employees. The current master policies are published at https://policy.ceresti.com.
    - The Security Officer communicates policy changes to all employees via email. These emails include a high-level description of the policy change using terminology appropriate for the target audience.
5. All policies, and associated documentation, are retained for 5 years from the date of its creation or the date when it last was in effect, whichever is later
    1. Version history and backup of all Ceresti policies is done via GitHub.
6. The policies and information security policies are reviewed and audited annually, or after significant changes occur to Ceresti's organizational environment. Issues that come up as part of this process are reviewed by Ceresti management to assure all risks and potential gaps are mitigated and/or fully addressed. The process for reviewing polices is outlined below:
    1. The Security Officer initiates the policy review by creating an Issue in the Ceresti Quality Management System.
    2. The Security Officer or the Privacy Officer is assigned to review the current Ceresti policies (https://policy.Ceresti.com/).
    3. If changes are made, the above process is used. All changes are documented in the Issue.
    4. Once the review is completed, the Security Officer or Privacy Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.
    5. If the review is approved, the Security Officer or Privacy Officer then marks the Issue as Done, adding any pertinent notes required.
    6. Policy review is monitored on a quarterly basis using the Quality Management System reporting to assess compliance with above policy.
7. Ceresti utilizes the HITRUST MyCSF framework to track compliance with the HITRUST CSF on an annual basis. Ceresti also tracks compliance with HIPAA and publishes results at https://hipaa.Ceresti.com. In order to track and measure adherence on an annual basis, Ceresti uses the following process to track HITRUST audits, both full and interim:
    1. The Security Officer initiates the HITRUST audit activity by creating an Issue in the Ceresti Quality Management System.
    2. The Security Officer or the Privacy Officer is assigned to own and manage the HITRUST activity.
    3. Once the HITRUST activity is completed, the Security Officer approves or rejects the Issue.
    4. If the review is approved, the Security Officer then marks the Issue as Done,

adding any pertinent notes required.

5. Compliance with annual compliance assessments, utilizing the HITRUST CSF as a framework, is monitored on a quarterly basis using the Quality Management System reporting to assess compliance with above policy.

Additional documentation related to maintenance of policies is outlined in §4.3.1.