Data Protection

`{{defaultRevision}}`

{{companyShortName}} takes the confidentiality and integrity of its customer data very seriously. As stewards and partners of {{companyShortName}} Customers, we strive to assure data is protected from unauthorized access and that it is available when needed. The following policies drive many of our procedures and technical controls in support of the {{companyShortName}} mission of data protection.

Production systems that create, receive, store, or transmit Customer data (hereafter "Production Systems") must follow the requirements and guidelines described in this section.

Policy Statements

{{companyShortName}} policy requires that:

(a) Data must be handled and protected according to its classification requirements and following approved encryption standards, if applicable.

(b) Whenever possible, store data of the same classification in a given data repository and avoid mixing sensitive and non-sensitive data in the same repository. Security controls, including authentication, authorization, data encryption, and auditing, should be applied according to the highest classification of data in a given repository.

(c) Workforce members shall not have direct administrative access to production data during normal business operations. Exceptions include emergency operations such as forensic analysis and manual disaster recovery.

(d) All Production Systems must disable services that are not required to achieve the business purpose or function of the system.

(e) All access to Production Systems must be logged, following the {{companyShortName}} Auditing Policy.

(f) All Production Systems must have security monitoring enabled, including activity and file integrity monitoring, vulnerability scanning, and/or malware detection, as applicable.