Text

Description automatically generated

|  |  |
| --- | --- |
| **Title:** Datasecuritypolicy | |
| **Department:** IT | **Version:** Original |
| **Approved by:** | **Approval date:** |
| **Senior management approval:** | |
| **Effective date:** | **Last updated:** |
| **Author:** | |
| **Scope**  This policy applies to all data and information activities that occur within <company name> and the data security activities that must be performed to protect data and information. | |
| **Responsibility**  The IT Department of <company name> is responsible for managing, upgrading and maintaining the elements and components of the company's computing environment including, but not limited to, all hardware, systems, data, databases, associated peripheral devices, and primary and secondary software applications.  The IT Department is also responsible for maintaining and updating this policy with the approval of the <enter title> and <enter title>. | |
| **Objectives**  The objective of this policy is to ensure the security and protection of data, databases and other data resources used by the company. This includes establishing and maintaining the confidentiality, integrity and availability of data needed by <company name> to conduct its business. | |
| **Strategy and focus**  <Company name>'s primary strategy for IT data security is to ensure <company name>'s data resources are secure, have appropriate access controls, have procedures to identify and prevent unauthorized access to <company name> data and databases, whether locally accessed or stored in managed services, such as cloud storage, and are aligned with the principles as stated in the standards ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-53, FISMA and HIPAA.  This policy addresses all IT data security activities at <company name>, including data files, databases and all electronic data elements within the IT computing environment. | |
| **Policy**  The confidentiality, integrity and availability of all company data, databases and other information resources are to be managed by a formal information data security program. This program will provide a controlled and orderly method by which access to <company name> data is requested and granted, security of data is monitored and analyzed, violations of data security are addressed and mitigated and changes to data security systems and procedures are requested, tested, approved and communicated for audit and recordkeeping purposes.  The following are required data security processes:   1. The IT department will define data security processes and procedures; secure and use specialized software and systems to reduce the threat of data security breaches; regularly test the security of the company's perimeters using penetration tests and other forensic methods; and document all data security procedures and controls. 2. The IT department will periodically conduct a risk assessment of the internal and external threats and vulnerabilities of <company name>'s data security environment. 3. Data security policies and associated activities will comply with legislative, regulatory and contractual requirements. 4. The IT department will provide data security education, training and awareness programs. 5. The IT department will enable disaster recovery capabilities in its data security controls. 6. The IT department will define the consequences of violating the data security policy. 7. The IT department will define how data security incidents are reported and managed. 8. Data in use at <company name>, whether at rest or in motion, must be encrypted. 9. <Company name> employees must sign the employee contract agreeing to accept and comply with data security policies at the time they are hired and on a regular basis (e.g., annually) through the employee handbook and/or in contract renewals to account for policy changes over time. 10. All proposed changes to data security are to be documented in detail. | |
| **Additional policies**  Additional policies that are part of <company name>'s overall data security policy may include, at management's discretion, the following:   * **Data classification** -- Describes specific classifications of data, the levels of control at each level and the responsibilities of all potential users. * **Acceptable use** -- Describes the organizational permissions for the use of IT and information-related resources. * **End-user computing** -- Describes the parameters and use of desktop, mobile computing and other tools by <company name> employees. * **Access control** -- Describes the method for defining and granting access to data resources to employees. | |
| **Applicability of other policies**  This document is part of <company name>'s suite of IT policies. Other policies may apply to the topics covered in this document, and as such, the applicable policies should be reviewed as needed. | |
| **Enforcement**  This policy will be enforced by the IT department in partnership with the HR department. | |
| **Management and audit review**  IT management will review and update IT policies on a quarterly basis and may launch a change management initiative to change the policy(ies). All <company name> IT policies will be available for review during scheduled IT audits. | |