Text

Description automatically generated

|  |  |
| --- | --- |
| **Title:** Shadow ITpolicy | |
| **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 operational and security activities that must be performed to prevent, identify, address and mitigate shadow IT activities. | |
| **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>, <enter title> and <enter title>. | |
| **Objectives**  The objective of this policy is to ensure shadow IT activities affecting the protection and security of operations, data, databases, networking, environmental and other IT resources used by the company are prevented, identified, addressed and mitigated. This policy integrates with and complements existing policies and procedures addressing IT operations, physical and logical security, and other operational activities needed by <company> to conduct its business. | |
| **Strategy and focus**  <Company name>'s primary strategy for addressing shadow activities is multipronged. Using and complementing existing policies and procedures for IT operations and security, this policy ensures <company name>'s data resources and operations are secure, have appropriate access and security controls, and have procedures to identify and prevent unauthorized access to <company name> systems, networks, data and databases. This includes operations and resources that may be locally accessed in a physical data center or implemented on technology platforms in managed services, such as cloud technology, and are aligned with the principles presented in global information security standards ISO/IEC 27001 and ISO/IEC 27002 and U.S. standards NIST SP 800-53, FISMA and HIPAA (data security).  This policy addresses all IT operational and networking activities, data resources, physical and logical security, and employees at <company name> within the IT computing environment. | |
| **Policy**  The confidentiality, integrity and availability of company IT operations, networking, data, databases and other information resources are to be protected from unauthorized shadow IT attacks via a coordinated program using existing security policies and procedures, partnering with other company departments (for example, HR and legal) and procedures to quickly identify suspicious activity, respond to the activity and mitigate it from causing any damage to IT operations. The shadow IT initiative can be standalone or part of existing IT security activities. The program will provide a controlled and orderly method by which suspicious IT activities are identified and mitigated, with specific post-event procedures for dealing with the perpetrator(s) of the attack.  The following actions must be developed into procedures that respond to shadow IT events:   1. The IT department will define processes and procedures to identify, address and mitigate suspected shadow IT activities. 2. The IT department will consider using specialized software and systems to reduce the threat of shadow IT activities by identifying suspicious activity and providing evidence of that activity. 3. The IT department will include a discussion of suspected shadow IT activities during daily, weekly and/or monthly meetings. 4. The IT department will regularly test the security of the company’s network perimeters using penetration tests and other forensic methods and document all procedures and controls with an emphasis on shadow IT. 5. The IT department will periodically test the physical security (for example, data center access) with an emphasis on shadow IT. 6. The IT department will include shadow IT considerations when it reviews and tests its controls for physical and logical security access. 7. The IT department will periodically liaise with HR and legal departments on shadow IT issues. 8. The IT department will periodically conduct a risk assessment of the internal and external threats and vulnerabilities (including shadow IT) of the <company name> IT operations and security environment. 9. The IT department will provide education, training and awareness of shadow IT activity. 10. The IT department will ensure technology disaster recovery capabilities will be initiated in a shadow IT attack, if needed. 11. The IT department, in partnership with HR, legal and other relevant departments, will define consequences of identified and confirmed shadow IT activity. 12. The IT department will define how shadow IT incidents are reported and managed. 13. <company name> employees and approved contractors must sign an agreement to comply with data security and operational security policies at the time they are hired and on a regular basis (for example, annually). 14. Shadow IT and related security policies and associated activities will comply with stated legislative, regulatory and contractual requirements. 15. The IT department will document all activities relating to shadow IT for management and audit review. | |
| **Additional policies**  Additional policies that are part of <company name>’s overall physical and logical security policies may include, at management’s discretion, the following:  **Acceptable use.** Describes the organizational permissions for the usage of IT and information-related resources.  **End-user computing.** Describes the parameters and usage 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 <company name> 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 and legal departments. | |
| **Management and audit review**  IT management will review and update IT policies on a quarterly basis at <company name>. As changes to IT policies are indicated in the course of business, IT management may launch a change management initiative to change the policies. All <company name> IT policies will be available for review in the course of scheduled IT audits. | |
|  | |