**Text

Description automatically generated**

**Remote access security policy template**

|  |  |
| --- | --- |
| **Title:** Remote access security policy | |
| **Department:** | **Version:** Original |
| **Approved by:** | **Approval date:** |
| **Senior management approval:** | |
| **Effective date:** | **Last updated:** |
| **Author:** | |
| **Scope**  This policy applies to the <specify location> of <company name>, <address>. | |
| **Authority**  This policy is hereby approved and authorized.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Name Title Date  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Name Title Date | |
| **Purpose**  The purpose of this policy is to define the activities associated with the provision of access security for employees and authorized nonemployees working remotely to protect <company name> information systems, networks, data, databases and other information assets from cybersecurity events that may occur while in use by remote workers. Additional policies governing data protection activities will be addressed separately. | |
| **Scope**  The scope of this remote access security policy is all IT systems, software, databases, applications and network resources needed by the Company to conduct its business, and the access security controls needed to protect those assets when being accessed remotely. The policy is applicable to all Company employees, contractors and other authorized third-party organizations. | |
| **Statement of compliance**  This policy is designed to be compliant with the U.K. Data Protection Act of 1998, U.K. Freedom of Information Act of 2000, U.S. Fair and Accurate Credit Transactions Act of 2003, U.S. Gramm-Leach-Bliley Act, Personal Information Protection and Electronic Documents Act in Canada and Europe's GDPR. It is designed to be consistent with information security standards and guidance, including ISO 27001 (Information Security Management Systems -- Requirements) and NIST SP 800-53 (Security and Privacy Controls).  Remote access security policy compliance is managed by the IT department, with support from <company name> department leadership and subject matter experts. To achieve compliance, remote access security programs must include appropriate procedures and security controls, as well as identify staffing and technology resources to meet compliance requirements. Compliance verification is performed monthly by the IT department, internal audit or other appropriate entity. | |
| **Policy**  The IT department is responsible for managing all remote access security activities for the Company. Other departments in the Company are responsible for providing the IT department with their requirements for remote access and security by employees, contractors and other authorized third parties. The IT department is responsible for developing, executing and periodically testing remote access security procedures. The IT department also acknowledges it will comply with appropriate industry standards for remote access security in its activities.   1. The company shall develop comprehensive remote access and security procedures and implement relevant secure remote access technology to all authorized employees, contractors and third parties in accordance with good cybersecurity and data protection practices as defined by established standards. 2. Remote access security activities shall be performed as part of the Company's cybersecurity and data protection programs, which include the following:    * planning and design of remote access security programs, plans and procedures;    * determining who is eligible for remote access to Company information resources;    * defining confidentiality, integrity and availability controls for remote access users;    * defining, evaluating, selecting and implementing technology resources to ensure remote access security to authorized users;    * identifying remote access security teams, defining their roles and responsibilities, and ensuring they are properly trained and prepared to perform their duties;    * scheduling of updates to remote access security policies and procedures;    * monitoring and analysis of remote access data traffic to identify possible security anomalies;    * planning and delivery of awareness and training activities for employees and remote access security team members;    * planning and execution of remote access security program and technology exercises;    * designing and implementing remote access security maintenance activities to ensure that plans, procedures and security technologies are current and ready for use;    * preparing for management review and auditing of remote access security controls and plan(s); and    * planning and implementation of continuous improvement activities for remote access security activities and plans. 3. Formal risk assessments and business impact analyses associated with operational resilience programs shall include requirements for remote access security. 4. Remote access security procedures shall support approved access controls, including authentication rules, role-based access and data encryption. 5. Remote access security plans and procedures shall be periodically reviewed and tested in a suitable environment to ensure that security on all remotely accessed sessions is provided and that Company management and employees know how to execute security controls and understand their roles and responsibilities for protecting Company information resources. 6. All external contractors and authorized third parties are made aware of the remote access security program and their own roles and responsibilities. 7. This remote access security policy, along with remote access security plans and procedures, are to be kept up to date and will be revised using change management to reflect changing circumstances. | |
| **Remote access security specifications**  **General**   1. State the frequency and types of remote access security activities to be performed. 2. State who is eligible for remote access to Company information resources. 3. State who should be notified if a problem with remote access security is identified.   **Remote access procedures**   1. State how remotely located systems access Company IT resources. 2. State how secure remote sessions are established and terminated. 3. State process for ensuring that remote access security controls work properly. 4. State process for validation of remote access security controls. 5. State process for monitoring remote access data traffic and identifying security issues. 6. State process for a remote user to obtain technical support for a remote access security issue. | |
| **Policy leadership**  **<Title of executive>** is designated as the corporate owner responsible for remote access security activities for the Company. Identification and resolution of remote access security issues should be coordinated with IT management and others as needed. | |
| **Policy responsibilities**   * Policy approval: The **<title of executive>** is responsible for approving this policy. * Policy implementation: The <enter name of department or individual> is responsible for planning, organizing and implementing all activities that fulfill this policy. * Policy maintenance and updating: The <enter name of department or individual> is responsible for all activities associated with maintaining and updating this policy. * Policy monitoring and review: The <enter name of department or individual> is responsible for monitoring and reviewing this policy. * Policy improvement: The <enter name of department or individual> is responsible for defining and implementing activities that will improve this policy. | |
| **Management review**  <Enter name of department or individual> will review and update this remote access security policy on an annual basis. As changes to this policy are indicated in the course of business, <enter name of department or individual> may initiate a change management process to update this policy. | |
| **Policy enforcement**  The **<title of executive>** will enforce this policy. | |
| **Penalties for noncompliance**  In situations where it is determined that remote access security activities performed by one or more remote users do not comply with this policy, the IT department team assigned to this activity will prepare a report stating the reason(s) for noncompliance and present it to IT management for resolution. Failure to comply with this remote access security policy within the allotted time for resolution may result in verbal reprimands, notes in personnel files, termination and such other remedies as deemed appropriate. | |
| **Policy location**  The policy will be signed, scanned into an electronic file and posted in the following location on the network: <enter location of policy>. | |