Chameleon

Security

Remote Access Policy

Purpose

The purpose of this policy is to establish comprehensive guidelines and procedures for remote access to company networks, systems, and data, ensuring the confidentiality, integrity, and availability of information assets. By following this policy, the company aims to mitigate the risks associated with remote access while enabling authorised users to perform their job duties efficiently and securely. This policy aligns with Australian laws and regulations, including the Privacy Act, and industry standards such as ISO 27002:2022 Control 6.7 – Remote Working, to safeguard sensitive data and maintain the trust of customers and stakeholders.

Scope

This policy applies to all employees, contractors, and third-party users who require remote access to company resources, regardless of their location. It covers all devices and methods used for remote access, including laptops, mobile devices, and virtual private networks (VPNs). Additionally, the policy extends to all company-owned or BYOD devices used for remote access, ensuring consistency and uniformity in security measures across the organisation.

Policy Compliance

Compliance with this policy is mandatory for all individuals accessing company resources remotely. Non-compliance may result in disciplinary action in accordance with company policies and may also violate Australian laws and regulations.

Definitions

Remote Access:

Remote access refers to the ability of authorised users to connect to the company's network, systems, and data from a location outside the corporate premises. This includes accessing resources such as files, applications, and email services using approved methods and devices.

Authorised Users:

Authorised users are individuals who have been granted permission by the company to access its network and resources remotely. This includes employees, contractors, and third-party users who require remote access to perform their job duties.

Remote Access Technologies:

Approved methods used to facilitate remote access, including VPNs, remote desktop services, and cloud-based solutions.

VPN(Virtual Private Network):

A VPN is a secure network connection that enables users to access the company's network securely over the internet. It encrypts data transmitted between the user's device and the company's network, ensuring confidentiality and integrity.

Remote Desktop Services:

Remote Desktop Services (RDS) allow users to access desktops and applications hosted on remote servers. It provides a graphical interface for users to interact with remote systems as if they were physically present at the office.

BYOD (Bring Your Own Device):

BYOD refers to the policy that allows employees to use their personal devices, such as laptops, smartphones, and tablets, for work purposes. These devices may be used for remote access to company resources but must adhere to security requirements outlined in this policy.

Multi-Factor Authentication (MFA):

Multi-Factor Authentication is a security mechanism that requires users to provide multiple forms of verification before gaining access to a system or application. This typically involves something the user knows (e.g., a password) and something the user has (e.g., a token or biometric identifier).

Endpoint Security:

Endpoint security refers to the protection of devices such as laptops, smartphones, and tablets from cybersecurity threats. It includes measures such as antivirus software, firewalls, and encryption to secure endpoints against malware, data breaches, and unauthorised access.

Data Encryption:

Data encryption is the process of encoding data to make it unreadable to unauthorised users. It ensures the confidentiality of data transmitted over the internet or stored on remote devices by converting it into ciphertext that can only be decrypted with the appropriate key.

Session Timeout:

Session timeout is a security feature that automatically logs out users from remote access sessions after a period of inactivity. This helps prevent unauthorised access to sensitive information if a device is left unattended.

Incident Reporting:

Incident reporting refers to the process of notifying appropriate personnel about security incidents or suspected security breaches. It enables prompt investigation and response to mitigate the impact of incidents on the company's information assets.

Policy Statement

Overview of Remote Access:

Remote access is provided to authorised users to facilitate business operations from locations outside the corporate network. This policy governs the use of remote access technologies and outlines security measures to protect company resources from unauthorised access and cyber threats. The company acknowledges the importance of enabling remote work flexibility while prioritising the security of its information assets.

Authorised Remote Access Methods:

Only approved methods such as VPNs and remote desktop services are allowed for remote access. Users must adhere to company policies and procedures when accessing company resources remotely. Any unauthorised methods, including unsecured public Wi-Fi networks and personal devices, are strictly prohibited to prevent potential security breaches.

Prohibited Remote Access Methods:

Unauthorised methods, including unsecured public Wi-Fi networks and personal devices, are strictly prohibited. This ensures that remote access is conducted in a secure manner and reduces the risk of unauthorised access to company resources.

Responsibilities of Authorised Users:

Authorised users are responsible for securing their remote access devices and reporting any suspicious activity. They must comply with Australian laws and regulations, including the Privacy Act and the Australian Government Information Security Manual (ISM), to ensure the confidentiality, integrity, and availability of company information.

Compliance with Legal and Regulatory Requirements:

The Remote Access Policy complies with relevant Australian laws, regulations, and industry standards, including but not limited to the Privacy Act and ISO/IEC 27001. This ensures that the company operates within the legal framework and maintains the privacy and security of sensitive data.

Access Control

- **Authentication Requirements:**

Remote access users must authenticate using strong, multi-factor authentication methods, following ISO 27002:2022 Control 6.7.2 – Secure Log-on Procedures. This includes complying with Australian Government Authentication Credential Management (AGACM) requirements.

- **Authorisation Procedures:**

Access to company resources is granted based on the principle of least privilege, following ISO 27002:2022 Control 6.7.4 – Access Control Policy. Users must have appropriate authorisations in accordance with their roles and responsibilities.

- **Multi-factor Authentication (MFA):**

MFA is mandatory for all remote access sessions to provide an additional layer of security, following ISO 27002:2022 Control 6.7.2 – Secure Log-on Procedures and AGACM requirements.

- **Session Timeout:**

Remote access sessions should have an automatic timeout mechanism to terminate inactive sessions and reduce the risk of unauthorised access, following ISO 27002:2022 Control 6.7.2 – Secure Log-on Procedures.

Security Measures

- **Encryption Standards:**

All remote access sessions must be encrypted using industry-standard protocols (e.g., TLS) to protect data confidentiality, following ISO 27002:2022 Control 6.7.1 – Cryptographic Controls and Australian Government Encryption Controls.

- **VPN Requirements:**

VPNs must be used for all remote access sessions to establish secure and encrypted connections, following ISO 27002:2022 Control 6.7.5 – Network Security Zoning and AGACM requirements.

- **Firewall Configuration:**

Firewalls must be configured to restrict unauthorised access to company networks and systems, following ISO 27002:2022 Control 6.7.5 – Network Security Zoning and Australian Cyber Security Centre (ACSC) guidelines.

- **Antivirus and Malware Protection:**

Remote access devices must have up-to-date antivirus and anti-malware software installed, following ISO 27002:2022 Control 6.7.6 – Malware Protection and ACSC recommendations.

- **Endpoint Security:**

Remote access devices should have endpoint security solutions installed to prevent unauthorised access and protect against malware infections, following ISO 27002:2022 Control 6.7.6 – Malware Protection and ACSC guidelines.

Device Security

- **Approved Devices for Remote Access:**

Only company-approved devices meeting security standards are allowed to connect remotely, following ISO 27002:2022 Control 6.7.3 – Mobile Device Security and ACSC guidelines.

- **Bring Your Own Device (BYOD) Policy:**

BYOD is permitted only if devices meet company security standards and are registered with the IT department, following ISO 27002:2022 Control 6.7.3 – Mobile Device Security and AGACM requirements.

- **Device Management and Configuration:**

Remote access devices must be regularly patched and updated to address security vulnerabilities, following ISO 27002:2022 Control 6.7.3 – Mobile Device Security and ACSC recommendations.

- **Lost or Stolen Device Procedures:**

Procedures must be in place for reporting and deactivating remote access on lost or stolen devices to prevent unauthorised access to company resources, following ISO 27002:2022 Control 6.7.3 – Mobile Device Security and ACSC guidelines.

Data Security

- **Data Encryption:**

All data transmitted during remote access sessions must be encrypted, and sensitive data stored on remote devices must be encrypted at rest, following ISO 27002:2022 Control 6.7.1 – Cryptographic Controls and Australian Government Encryption Controls.

- **Data Backup and Recovery:**

Data accessed remotely must be backed up regularly to prevent data loss, following ISO 27002:2022 Control 6.7.8 – Data Back-up and ACSC guidelines.

- **Data Access Controls:**

Access to sensitive company data must be restricted based on user roles and responsibilities, following ISO 27002:2022 Control 6.7.4 – Access Control Policy and Australian Privacy Principles.

Monitoring and Reporting

- **Remote Access Activity Monitoring:**

Remote access activity must be monitored regularly for unauthorised access attempts or suspicious activity, following ISO 27002:2022 Control 6.7.7 – Monitoring and ACSC recommendations.

- **Incident Response Procedures:**

Procedures must be in place for responding to security incidents related to remote access, including reporting, investigation, and remediation, following ISO 27002:2022 Control 6.7.7 – Monitoring and ACSC guidelines.

Training and Awareness

- **Remote Access Training:**

All remote access users must receive training on the company's remote access policies, procedures, and best practices, following ISO 27002:2022 Control 6.7.9 – Security Awareness, Education, and Training and ACSC recommendations.

- **Security Awareness Programs:**

Ongoing security awareness programs must be conducted to educate remote access users about cybersecurity risks and best practices, following ISO 27002:2022 Control 6.7.9 – Security Awareness, Education, and Training and ACSC guidelines.

Compliance and Legal Considerations

- **Legal Compliance:**

The Remote Access Policy shall adhere to relevant Australian laws, regulations, and industry standards, including but not limited to the Privacy Act and ISO/IEC 27001.

- **Recordkeeping:**

Records and documentation related to remote access policies, procedures, and audit trails shall be maintained in accordance with legal and regulatory requirements.

Policy Review and Maintenance

- **Annual Review:**

The Remote Access Policy shall be reviewed annually or more frequently as needed to ensure its effectiveness, relevance, and alignment with changing business requirements and regulatory standards.

- **Change Management:**

Procedures shall be established for implementing changes to the Remote Access Policy, including approval, testing, and communication to affected parties.

Enforcement and Compliance

- **Enforcement Mechanisms:**

Compliance with the Remote Access Policy shall be enforced through monitoring, audits, and disciplinary actions for non-compliance.

- **Consequences of Non-Compliance:**

Violations of the Remote Access Policy shall result in appropriate consequences, including warnings, sanctions, and termination of access privileges.

- **Reporting Procedures:**

Mechanisms shall be in place for users to report suspected violations of the Remote Access Policy, ensuring timely investigation and resolution.

Appendices

Appendix A: Remote Access Approval Form

This form must be completed and submitted by employees requesting remote access to company resources. It includes details such as the employee's name, department, reason for remote access, and approval from the appropriate manager or supervisor.

Appendix B: Remote Access Configuration Guide

This guide provides instructions for configuring remote access tools and VPN clients to connect securely to the company network. It includes step-by-step procedures for different operating systems and devices, along with best practices for ensuring security during remote access sessions.

Appendix C: Remote Access Acceptable Use Policy

The acceptable use policy outlines guidelines and restrictions for remote access to company resources. It covers topics such as permissible activities, prohibited behaviours, and consequences for violating the policy. Employees are required to read and acknowledge this policy before accessing company systems remotely.

Appendix D: Incident Reporting Procedure

This document outlines the procedure for reporting security incidents related to remote access. It includes contact information for the IT security team, details on what constitutes a security incident, and steps to take if an incident is suspected or detected during remote access sessions.

Appendix E: Remote Access Training Materials

Training materials provide employees with information on how to use remote access tools securely and responsibly. This may include e-learning modules, instructional videos, or written guides covering topics such as password management, data encryption, and safe browsing practices.

Appendix F: Remote Access Policy Acknowledgement Form

Employees are required to acknowledge their understanding and acceptance of the remote access policy by signing this form. It serves as evidence that employees have read and agreed to comply with the policy's requirements and guidelines.

Appendix G: Glossary of Terms

A glossary provides definitions for technical terms and acronyms used throughout the remote access policy. It helps ensure clarity and consistency in understanding key concepts related to remote access and cybersecurity.