Cyber Security Policy

Prepared by: Cyber Security Officer

Issue Date: 19/03/2025

Version: 2.0

Approved by

General Manager

Jamal Kubeer

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Contents

Introduction

In our current fast-paced digital landscape, safeguarding our organization's digital assets is paramount. This cybersecurity policy serves as our blueprint for maintaining the security and integrity of our digital infrastructure. By adhering to these guidelines and remaining vigilant, we fortify our defenses against cyber threats, ensuring the resilience and continuity of our operations.

Purpose

Our company's cybersecurity policy serves as a comprehensive framework outlining our guidelines and provisions for safeguarding the security of our data and technology infrastructure. In today's increasingly interconnected digital landscape, the protection of our sensitive information is paramount. We have implemented a multitude of security measures to defend against both external and internal threats, recognizing the potential financial and reputational damage that breaches may inflict. Within this policy, we have articulated detailed instructions aimed at mitigating security risks and ensuring the integrity of our organization's assets.

Scope

The policy applies to all our employees, stakeholders, contractors, and anyone who has permanent or temporary access to our systems and hardware.

Policy Elements

1. Confidential data

Confidential data refers to information whose unauthorized use, disclosure, acquisition, modification, loss, or deletion could result in significant harm to the company, its partners, and customers. Examples of confidential data include, but are not limited to:

- Unpublished financial information
- Customer, partner, and vendor data
- Human resources records
- Records related to vouchers and gift cards
- Protecting this data is essential to maintain the trust and integrity of our organization and its relationships with stakeholders.

Protecting this data is essential to maintain the trust and integrity of our organization and its relationships with stakeholders.

2. Protect company devices

The security of our company's data is of utmost importance, and it relies heavily on the adherence of employees to cybersecurity protocols. The following guidelines aim to mitigate risks and prevent data leakage associated with the use of digital devices:

- **Device Usage:** Employees must exclusively access their work emails and internal systems using company-issued devices. This practice ensures

consistent application of security measures and minimizes the risk of unauthorized access.

- **Personal Use Restrictions:** Employees are prohibited from using company devices and equipment to access personal emails or web accounts. Such usage introduces vulnerabilities and compromises the integrity of our systems.

- **Password Protection:** It is essential for all devices to be password-protected to prevent unauthorized access. Employees must adhere to password policies and regularly update their credentials.

- **Device Security:** Employees should never leave their devices exposed or unattended, especially in public areas. Proper physical security measures must be maintained at all times to prevent unauthorized access.

- **Avoid Sharing Devices:** Employees are strongly advised against accessing company external or internal systems (via VPN) from devices belonging to others or lending their devices to others. This precautionary measure reduces the risk of unauthorized access and ensures the integrity of our data.

3. Email Security measures

Emails are common targets for scams and malicious software, such as malware or viruses. To protect against potential infections or data theft, we advise our employees to adhere to the following guidelines:

- **Exercise caution with Attachments and Links:**
  Avoid opening attachments or clicking on links in emails when the content is not clearly explained. For example, refrain from clicking on links requesting actions like resetting passwords unless explicitly requested through official channels.

- **Beware of Clickbait Titles:**
  Be wary of emails with clickbait titles, such as those urging you to click on "unsubscribe" links. These tactics are often used by attackers to trick users into compromising their security.

- **Verify Senfer Information:**
  Always verify the email address and name of the sender before interacting with the message. If the sender's identity seems suspicious or unfamiliar, exercise caution and refrain from taking any action.

- **Exercise Discretion with File Downloads:**

Refrain from downloading any files attached to emails unless you are certain that the sender is legitimate. Exercise caution, particularly with unexpected or unsolicited file attachments.

Please note that while proper security monitoring and filtering for viruses are applied on the domain gateway, it's essential to remain vigilant and adhere to these guidelines to further enhance our email security measures. If an employee is uncertain about the safety of an email they've received, they should immediately contact our IT/Cybersecurity department for assistance and guidance. Your vigilance and adherence to these guidelines are critical in maintaining the security of our organization's data and systems.

4. Effective Password Management

Password leaks pose significant risks as they can compromise user accounts and devices, potentially leading to breaches in data integrity, data theft, and ransomware attacks. To mitigate these risks, employees should strictly adhere to the following guidelines:

- **Create Strong Passwords:**
  Choose passwords with a minimum of 10 characters, incorporating a combination of upper-case letters, lower-case letters, numbers, and symbols. Strong passwords are essential for enhancing the security of user accounts and preventing unauthorized access.

- **Avoid Writing Down Passwords:**
  Refrain from writing passwords down and storing them in easily accessible locations, such as desks or office clipboards. Written passwords pose a security risk if they fall into the wrong hands and can compromise the confidentiality of user accounts.

- **Avoid Sharing Credentials:**
  Avoid sharing login credentials with colleagues for any tasks or purposes. Each employee should be responsible for safeguarding their own credentials to prevent unauthorized access and maintain accountability for their actions.

- **Use Unique Passwords for Each Account:**
  Avoid using the same password for multiple accounts. Using unique passwords for each account helps mitigate the impact of potential security breaches, as compromising one account does not compromise others.

- **Change Passwords Regularly:**
  Change passwords every 3 months to enhance security. Regular password changes reduce the risk of unauthorized access and help mitigate the impact of potential security breaches.

By adhering to these guidelines, employees contribute to strengthening the overall security posture of our organization and reducing the risk of password-related security incidents. Your commitment to password security is crucial in safeguarding our data and protecting against potential threats.

5. Transfer Data Securely

Transferring data introduces security risks, and employees must exercise caution to prevent unauthorized access and protect sensitive information. To mitigate these risks, employees should adhere to the following guidelines:

- **Minimize Data Transfers:**
  Avoid transferring sensitive data, such as customer information or employee records, to other devices or accounts unless absolutely necessary. In cases where mass transfer of such data is required, employees should seek assistance from our IT department for guidance and support.

- **Utilize Secure Channels:**
  Share confidential data exclusively over the company network/system rather than public Wi-Fi or private connections. Utilizing secure channels helps mitigate the risk of interception and unauthorized access to sensitive information.

- **Verify Recipient Authorization:**
  Before transferring data, ensure that recipients are properly authorized individuals or organizations with adequate security policies in place. Verifying recipient authorization helps maintain the confidentiality and integrity of the transferred data.

- **Report Security Incidents:**
  Promptly report any scams, privacy breaches, or hacking attempts to our IT Department. Early detection and reporting of security incidents are crucial for mitigating potential risks and preventing further data breaches.

- **Password Protected Documents:**
  Ensure that sensitive data is always protected with passwords. By password-protecting documents containing sensitive information, even if someone gains unauthorized access to the data, they will be unable to read it without the corresponding password. This additional layer of security helps safeguard sensitive information and mitigates the risk of unauthorized disclosure or access.

By adhering to these guidelines, employees play a vital role in safeguarding the confidentiality and integrity of our organization's data. Your diligence and adherence to these security measures contribute to maintaining a secure and resilient data environment.

6. Network Security

Misconfigured network and security devices within the infrastructure pose significant risks, potentially allowing hackers to exploit vulnerabilities and launch cyber-attacks. It is imperative for the Network and Security Administrator to adhere to the following guidelines to minimize the attack surface and maintain proper security controls, thereby strengthening the network and security of the company's infrastructure:

- **Regular Configuration Audits:**
  Conduct regular audits of network and security device configurations to identify and rectify any misconfigurations or vulnerabilities that could be exploited by attackers.

- **Implement Least Privilege Access:**
  Configure network and security devices to adhere to the principle of least privilege, granting users only the access permissions necessary to perform their roles and responsibilities.

- **Strong Authentication Mechanisms:**
  Implement strong authentication mechanisms, such as multi-factor authentication (MFA), to prevent unauthorized access to network devices and sensitive information.

- **Segmentation and Zoning:**
  Implement network segmentation and zoning to logically isolate different parts of the network, limiting the potential impact of security breaches and preventing lateral movement by attackers.

- **Regular Security Patching:**
  Ensure that network and security devices are regularly patched and updated with the latest security patches and firmware updates to address known vulnerabilities and reduce the risk of exploitation.

- **Incident Response Plan:**
  Develop and maintain an incident response plan outlining procedures for detecting, responding to, and recovering from network security incidents. Regularly test and update the plan to ensure its effectiveness in mitigating cyber threats.

- **Employee Training and Awareness:**
  Provide regular training and awareness programs for employees to educate them about common network security threats, best practices for secure network usage, and their roles and responsibilities in maintaining network security.

7. Endpoint Security

Endpoint security software, such as antivirus programs, plays a crucial role in protecting the endpoint devices within the company's environment from external threats. These software solutions continuously monitor the devices and scan for any new files added to the endpoints. In the absence of antivirus protection, endpoint devices become vulnerable to cyber threats, as malware and trojans can easily infiltrate the devices.

- **Ensure Antivirus Installation:**
  It is imperative to ensure that antivirus software is installed on every endpoint device connected to the network and containing company data. Antivirus protection helps detect and mitigate the risk of malware infections and other security threats.

- **Maintain Up-to-Date Antivirus:**
  Regularly update antivirus software to ensure it is equipped with the latest threat definitions and security patches. Continuous updates help enhance the effectiveness of antivirus protection and safeguard endpoint devices against emerging threats.

- **Regular Scanning and Monitoring:**
  Schedule regular scans of endpoint devices to detect and remove any existing malware or suspicious files. Additionally, implement continuous monitoring of endpoint activities to identify and respond to any security incidents in a timely manner.

8. Physical Security:

Physical security is paramount for safeguarding the network, security, and servers housed within the data center. The following measures must be strictly adhered to:

- **Restricted Access:**

Only authorized personnel with the appropriate clearance levels should have access to the data center. Access should be strictly controlled and monitored to prevent unauthorized entry.

- **Cable Labeling:**
  Label each network cable with clear and descriptive identifiers, such as the device name, port number. This will avoid down time by eliminating human error.

- **Logging Audit:**

Maintain a comprehensive log of every instance of check-in and check-out from the data center, including the time and identity of the personnel involved. This logging system ensures accountability and enables tracking of access to sensitive equipment and areas within the data center.

9. Monitoring and Audit:

Regular monitoring and audit of network infrastructure and security controls are essential for maintaining the integrity and effectiveness of the organization's cybersecurity measures. The following guidelines should be followed:

- **Monitoring:**
  Proactive monitoring of network traffic, system activities, and security events in real-time. This allows for the timely detection of security incidents and abnormal behavior.

- **Log Management:**
  Collect and retain logs from network devices, servers, and security systems to facilitate forensic analysis and compliance with regulatory requirements. Regularly review and analyze logs to identify security incidents and potential vulnerabilities.

- **Security Audit:**
  Conduct periodic security audits and assessments to evaluate the effectiveness of network security controls and identify areas for improvement. Utilize both internal and external audits to gain insights into the organization's security posture and compliance with industry standards.

Disciplinary Action

Violation may result in disciplinary action in according with company policy. Failure to observe these guidelines may result in disciplinary action by the company depending upon the type and severity of the violation, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s).

Policy Review

This policy is to be reviewed annually.

Signature

By signing below, I agree to the following terms:

I confirm that the above have read and received and read a copy of the "Cyber Security Policy" and agree to comply to it.

Full Name	Designation	Signature

Aashick . Noordine	Accountant	
Abdulrahman Mohamed ElRotel	Financial Manager	
Afif Hussein Mukahal	Executive Manager	
Ahmed Ahmed Soliman	Sales Executive	
Ahmed Ebraheem Mohamed Daloq	Logistics Officer	
Ahmed Hassan Al Gendy	Sales Executive	
Akhilesh Pokkanchery Vikramsingh	Senior Network Administrator	
Ali Khaleel Mohamed	Technical Support Engineer	
Amira Loka	Customer Support Officer	
Anto Oommen Chacko	Accountant	
Asmaa Metwally	Customer Support Officer	
Celda Castillo Zonio	Customer Support Officer	
Elsayed Mohammed Thabet	Risk Manager	
Fahim Mahamud Parkar	Mobile Developer	
Fatma Mohammed Alnasser	Sales Executive	
Hani Saad Radwan	Administration Officer	
Hany Hazem Diab	Logistics Officer	
Jamal Eldeen A. Kubeer	General Manager	
Jamal Mahmoud Ibrahim	Sales Executive	
Jinto Joy Joy	Internal Audit Manager	
Jobin Johnson Vaidyan	Accountant	
Khaled Al Ghunaim	Board Member	
Linto Lawrance Neelamkavil	Application Support Manager	
Mahmoud Ahmed Abdulhalim	Accountant	
Medhat Merzk Zaki Askander	Web Developer	
Michael Mansour Basily	Compliance Manager	
Mohamad Sameh Sbeiti	Customer Support Officer	
Mohamed Ahmad Nasr	Logistics Officer	
Mohamed Chisti	Network Administrator	
Mohamed Hassan A. Sanan	Logistics Officer	

Mohammad Mousa Al Shatti	Sales Executive	
Mohammed Sayed Sadek	Customer Support Officer	
Nesrine Zakaria Emam	HR & Administration Manager	
Omar Mahmoud Hagras	Project Manager	
Quadeer Mohammed Yousuf	Technical Support	Quadeer
Rama Krishna Uddarraju	Information Security Manager	
Razan Ibrahim Al Dalag	Customer Support Officer	
Realiza Usero Divina	Customer Support Officer	
Sabah Al Ghunaim	Chairman	
Salah Sayed Ahmad	Logistics Officer	
Sarah Sameh Sbeity	Customer Support Officer	Sara
Sayed ElSayed Tantawy	Customer Support Officer	
Shahad Abdulwahab Sawas	Software Tester	
Siju Abraham Oommen	Accountant	
Suku Mathew	Accountant	
Surya Satya	Logistics Officer	
Syed . Hussain	Net Developer	
Tawfek Shonoda Tawfek	Logistics Officer	