Network Security

Standards Document

Version 1

Produced:
March 10th, 2023

Edited:
April 19th, 2023

Written by:
Miguel Suárez - Security Officer
Alex Phillips - Director of infrastructure Expresia

Approved by:
Paula Amador - Chief Product Officer

1. Policy Statement

At Expresia, we recognize the importance of maintaining a secure network environment. We are committed to ensuring the confidentiality, integrity, and availability of our network infrastructure and data. We understand that cyber threats are constantly evolving, and therefore, it is imperative to have a comprehensive network security plan in place.

Our Network Security Standard outlines the guidelines and best practices to safeguard our network infrastructure, including our network devices, servers, workstations, and applications. We strive to stay up-to-date with the latest security trends and technologies to continuously enhance our security posture.

We understand that network security is a shared responsibility among all employees, contractors, and vendors who access our network. Therefore, we expect everyone to comply with our Network Security Standard and manage any suspected security incidents or vulnerabilities.

By following this Network Security Standard, we aim to minimize the risk of unauthorized access, data breaches, and other cyber threats.

2. Risk Assessment

To ensure the security of our network infrastructure, we conduct regular risk assessments to identify potential threats and vulnerabilities. The assessment includes an evaluation of our network architecture, devices, and applications that are in use. This helps us to identify potential risks, prioritize them based on their impact, and develop appropriate measures to mitigate them.

We use industry-standard risk assessment methodologies and tools to conduct our assessments, which include:

1. Asset Inventory: We maintain an up-to-date inventory of all network assets, including devices, software, and applications.
2. Threat Identification: We identify potential threats to our network infrastructure, such as malware, phishing attacks, and unauthorized access.
3. Vulnerability Assessment: We conduct regular vulnerability assessments to identify potential weaknesses in our network devices, servers, and applications.
4. Risk Analysis: We analyze the identified threats and vulnerabilities to determine their potential impact on our network infrastructure.
5. Risk Mitigation: We develop and implement appropriate measures to mitigate the identified risks based on their impact and likelihood.

By conducting regular risk assessments, we aim to proactively identify and mitigate potential security risks to our network infrastructure.

3. Access Control

Access control is a critical aspect of our Network Security Standard. We maintain strict controls that manage access to our network infrastructure and ensure that only authorized personnel can access our systems and data.

3.1. User Authentication and Authorization

To access our network infrastructure, users must be authenticated and authorized. We use strong password policies and Virtual Private Networks to ensure that only authorized users can access our network. All users are required to use a unique username and password.

3.2. Network Segmentation

We use network segmentation to partition our network infrastructure into smaller, more secure segments. This helps us to limit the potential impact of a security breach and contain any damage. We ensure that each segment is isolated from the other segments and only authorized personnel can access them.

4. Network Monitoring and Logging

We understand the importance of monitoring network traffic and logging events for analysis and auditing purposes. We maintain a comprehensive network monitoring and logging system.

4.1. Network Traffic Monitoring

We use network traffic monitoring tools to monitor our network infrastructure continuously. This helps us to detect potential incidents and suspicious activities in real-time. Any anomalies found, such as unusually high traffic volume (DDoS for example) or traffic patterns, that may indicate a security threat.

4.2. Logging and Event Management

We maintain a centralized logging system that collects and stores logs from all network devices, servers, and applications. This helps us to track and analyze network activities, detect potential security incidents, and investigate security breaches.

We also have an incident response plan in place to respond to security incidents promptly. The plan outlines the steps to be taken in the event of a security incident.

By implementing a comprehensive network monitoring and logging system, we aim to detect and respond to security incidents in a timely manner and maintain the confidentiality, integrity, and availability of our network infrastructure and data.

5. Data Protection

We take data protection seriously and have implemented several measures to protect data in transit on our network infrastructure. We ensure that our data is protected against unauthorized access, theft, or loss.

5.1. Encryption

To protect data in transit, we use strong encryption protocols, such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS), to encrypt data transmitted between our network devices, servers, and applications. We also use encryption technologies, such as Virtual Private Network (VPN), to create secure tunnels for remote access to our network infrastructure.

5.2. GDPR Compliance

In compliance with the General Data Protection Regulation (GDPR) of the European Union (EU), we ensure that all personal data transmitted over our network is encrypted using strong encryption protocols defined above. Our network infrastructure is regularly audited to ensure that it meets the GDPR's requirements for data protection.

5.3. Data Removal Requests Management

We have implemented procedures to manage data removal requests from individuals under the GDPR. These procedures include verifying the identity of the requester, locating and deleting the requested data, and providing confirmation of the deletion to the requester. We also maintain records of data removal requests and their outcomes to demonstrate compliance with the GDPR's requirements for data protection.

6. Patch Management

The Patch Management process is critical for maintaining a secure environment by addressing vulnerabilities in software applications and operating systems. The following procedures will be followed for managing and applying software patches and updates:

1. Identification of patches: The IT team will identify and review available patches and updates on a schedule, using sources such as vendor websites, security advisories, and industry publications. Patches will be classified based on their severity level, and their potential impact on the organization's systems and data. The severity level and impact assessment will be based on the affected service role and context, which will be documented and tracked accordingly.
2. Patch management plan: Based on the severity and impact assessment, a patch management plan will be developed for each patch. The plan will include a timeline for

patching, the resources required to patch the vulnerability, and the individuals responsible for patching.
3. Patch deployment: The IT team will deploy the patches according to the established timeline. This may involve testing the patch on a non-production system to ensure that it does not cause any issues before deploying it on production systems. All patching activities will be documented, and the status of each patch will be updated in the organization's patch tracking system.
4. Verification and validation: Once the patch has been deployed, the IT team will verify and validate that the patch has been successfully installed and that the vulnerability has been addressed. This may involve re-scanning the system or conducting other tests to confirm that the vulnerability is no longer present.
5. Rollback plan: In the event that a patch causes unexpected issues, the IT team will have a rollback plan in place to revert the system to its previous state. This will minimize the impact on the organization's systems and data.

By following these procedures, Expresia ensures software patches are promptly identified, assessed, and deployed to address vulnerabilities, reducing the risk of a security incident.

6.1. Network Software Update Policy

We have established a software update policy that requires all network devices and applications to be updated regularly to ensure they are running the latest software versions and security patches.

By implementing a comprehensive patch management program and software update policy, we aim to minimize the risk of security vulnerabilities and ensure the stability and reliability of our network infrastructure and applications.

7. Roles and Responsibilities

To ensure the effectiveness of our Network Security Standard, we have assigned the following roles and responsibilities:

1. Chief Technology Officer: The CTO is responsible for overseeing the development, implementation, and maintenance of the Network Security Standard. The CTO should ensure that the standard aligns with organizational objectives and is in compliance with regulatory requirements.
2. Expresia Technical Lead: The Technical Lead is responsible for ensuring that the standard is integrated into operational processes.
3. Director of Infrastructure: The Director of Infrastructure is responsible for ensuring that IT systems and infrastructure are configured following secure standards, as well as following the Network Security Standard in newer processes.
4. Security Officer: The Security Officer is responsible for working alongside the Technical Lead to ensure that current and future processes follow the Network Security Standard.
5. IT Support Specialist: The IT Support Specialist is responsible for identifying and reporting vulnerabilities to the Vulnerability Management team, and assists with testing.

6. Head of Human Resources: The Head of Human Resources is responsible for ensuring that employee awareness and training programs are in place to educate employees about the Network Security Standard.

Each role is critical to the success of our Network Security Standard, and we expect all employees to take their responsibilities seriously and actively contribute to maintaining the security and integrity of our network infrastructure.

8. Training and Awareness

Expresia recognizes that employee awareness and training are critical components of a successful Network Security Standard. We are committed to providing ongoing education and training to ensure that our employees are knowledgeable about the standard and their roles in executing it.

To achieve this, we will:

1. Develop and implement an employee training program that covers the Network Security Standard, including its objectives, policies, and procedures.
2. Provide regular training sessions to all employees to ensure that they are up-to-date on the latest security threats and risks, and are knowledgeable about best practices for protecting sensitive information.
3. Conduct periodic security awareness campaigns to reinforce the importance of security and the role that each employee plays in maintaining it.
4. Ensure that all new employees receive orientation training that covers the Network Security Standard, its policies, and their individual responsibilities.
5. Encourage employees to report any security concerns or incidents promptly, and to take an active role in protecting Expresia's network infrastructure.

By providing ongoing education and training, we aim to create a culture of security awareness and responsibility throughout the organization. We believe that this will help to reduce the risk of security breaches and ensure the continued protection of Expresia and customer data.