Newry, Mourne and Down District Council (NMD)

IT Policies

Contents

1. Purpose

This Policy dictates the various measures and limitations that are enforced on the User Accounts that are in use on NMD IT systems. This policy is applicable to the *Password Policy (IT-202).*

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

User Accounts are an important aspect of computer security. Users with access to NMD systems are responsible for securing their account details. If another user offers you an alternative Network Account, you **must** report this as a security incident to the IT Service Desk, or to the IT Department in person.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for the creation of strong passwords, the protection of those passwords, and the frequency of change.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Passwords are an important aspect of computer security. As such, each staff member with access to NMD systems is responsible to select and secure their own passwords. If someone demands or offers you a password, you **must** report this as a security incident to the IT Service Desk, or to the IT Department in person.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines NMD requirements to ensure that the network and systems are free from malicious software code. Anti-virus software protection includes the tools and procedures necessary to prevent major and widespread damage to user applications, files, and hardware, thus protecting the entire NMD Network.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as “electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software”.

3. Incident Reporting

New viruses are discovered almost every day and represent a significant threat to the security of NMD network. Any Anti-Virus security issues **must** be reported as a security incident immediately to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines NMD requirements for the secure disposal of assets containing sensitive data. The disposal of media, computer equipment, and computer software can create information security risks. These risks relate to the potential unauthorised disclosure of electronic data or intellectual property that could be stored in hard disks and other storage media.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Any security issues **must** be reported as a security incident immediately to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines NMD requirements to ensure that data (in the form of information assets) is retained according to legal, statutory and effective business requirements. This is to ensure that NMD meets its Legal Compliance obligations.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

All users of information assets in NMD are responsible for the security of all data and information they have access to. If you encounter any security issues you **must** report this as a security incident to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines the requirements to ensure that Email, (including Instant Messaging), is used in an appropriate manner taking into account the confidentiality and sensitivity of information being transmitted.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

If you receive any inappropriate or offensive material via email you **must** report this immediately to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for implementing security controls on the NMD Firewall. Firewalls can be complex to manage, and security incidents can occur daily. Without a policy to guide firewall implementation and administration, the firewall itself may become a security problem.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Any Firewall issues **must** be reported as a security incident immediately to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines the requirements to ensure that the Internet is used for appropriate mainly business purposes, protecting NMD reputation and keeping the Network and systems free from malicious software code.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

If when, accessing the Internet, you access a site that contains *offensive or inappropriate content*, you **must** report this as a security incident to the IT Service Desk, or in person to the IT Department. This Internet site can then be added to the category list of blocked sites.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for the acceptable use of IT equipment at NMD. Inappropriate use of IT equipment could expose NMD to risks including virus attacks, compromise of network systems and services, and legal issues. The Policy aims to protect both the employee and NMD.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Any IT Equipment security issues **must** be reported as a security incident immediately to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for patch management on the NMD network, ensuring all computer devices (including servers, desktops, printers, etc.) have secure virus protection software, current virus definition libraries, and the most recent operating system and security patches installed.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Any Patch security issues **must** be reported as a security incident immediately to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for local and network printing on NMD systems. These standards are designed to ensure the best possible support of the users, and to minimise the potential exposure of confidential prints such as Finance or Personnel records.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

All users of NMD printers are responsible for their confidential printed documents. If you encounter any security issues you **must** report this as a security incident to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for connecting to NMD network or systems from any remote host. These standards are designed to minimise the potential exposure to damage, which may result from unauthorised use of NMD resources.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Users with remote access to NMD Systems are responsible for securing their account details. If you encounter any security issues when connecting remotely, you **must** report this as a security incident to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for the use of Removable Media on all computers and servers operating in NMD or on customer sites. These standards are designed to minimise the risk of loss or exposure of sensitive information, and to reduce the risk of acquiring malicious software such as viruses.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Users with permission to use Removable Media on the NMD Network are responsible to secure their devices and information. If you encounter any security issues with Removable Media you **must** report this as a security incident to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for addressing IT Security Incidents that may occur on NMD network. Compromises in security can potentially occur at every level of computing from desktop computers to the best-protected systems. Regardless, each incident requires careful response with its potential impact to the security of NMD network and users.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Users **must** report any IT Security Incidents that may occur directly to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for the base configuration of internal server equipment that is owned and/or operated by NMD. Effective implementation of this policy will minimise unauthorised access to NMD proprietary information and technology.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Any Server Security issues **must** be reported as a security incident immediately to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

IT Policy – Server Space Usage Policy No: IT-304

1. Purpose

This Policy defines the requirements to ensure that Server Space is used in an appropriate manner taking into account the confidentiality and sensitivity of information stored on NMD Servers.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as “electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software”.

3. Incident Reporting

Users with allocated Server Space on NMD Servers are responsible to secure their access and data. If you encounter any security issues with Server Space you **must** report this as a security incident to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for software acceptance on the NMD network. This policy provides guidance to the IT Department relating to the use, compliance, and limits of copyrighted software.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

All suspected software violations **must** be reported as a security incident immediately to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for software installation and deployment on NMD network. This policy sets protocol as to how software is to be delivered to better enable the IT Department to achieve its objective of delivering stable, well-performing technology solutions.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

It is the responsibility of the IT Department to keep software licensing accurate and up to date. Any security issues **must** be reported as a security incident immediately to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards to ensure a secure method of network connectivity between NMD and all Third Parties. These standards are designed to minimise the potential exposure to damage, which may result from unauthorised use of NMD resources.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Users with Third Party Access **must** immediately report any incident or suspected incidents of unauthorised access to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines standards for wireless access to NMD network from any client or mobile device, (e.g. Tablet, laptop, etc.). These standards are designed to minimise the potential exposure to damage, which may result from unauthorised use of NMD resources.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Wireless access users **must** immediately report any incident or suspected incidents of unauthorised wireless access to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

The purpose of this policy is to establish a checklist of actions that **must be fully implemented** in the event that a person leaves the employment of NMD.

2. Scope

This Policy applies to all users of information assets to include NMD employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as “electronic and non-electronic assets owned by NMD or entrusted to NMD (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software”.

3. Incident Reporting

Taking the appropriate steps when an employee leaves is an important aspect of computer security. If someone who is leaving the employment of NMD asks for your help to circumvent any of the steps listed above, you **must** report this as a security incident to the IT Service Desk, or in person to the IT Department

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Purpose

This Policy defines the standards that will help you make appropriate decisions about your work-related blogging and the contents of your blogs, personal Web sites, postings on wikis and other interactive social media/networking sites[1], postings on video or picture sharing sites, or in the comments that you make online on blogs, elsewhere on the public Internet, and in responding to comments from posters either publicly or via email. **Our internal Internet Usage and Email Polices remain in effect in our workplace.**

NMD recognises the importance of the Internet in shaping public thinking about NMD and its current and potential services, employees, partners, and customers. NMD also recognises the importance of our employees joining in and helping shape public sector conversation and direction through blogging and interaction in social media. Therefore, NMD is committed to supporting your right to interact knowledgeably and socially in the blogosphere and on the Internet through blogging and interaction in social media.

These standards will help you to have a respectful, knowledgeable interaction with people on the Internet. They also protect the privacy, confidentiality, and interests of NMD and its current and potential services, employees, partners, and customers.

Note that these policies and guidelines apply only to work-related sites and issues and are not meant to infringe upon your personal interaction or commentary online.

2. Scope

This Policy applies to all NMD employees, employees of temporary employment agencies, and contractor personnel regardless of geographic location.

3. Incident Reporting

If you become aware of any breach of this policy, you **must** report this to the IT Service Desk, or in person to the IT Department.

4. Enforcement

It is the responsibility of the IT Manager to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

[1] Including, but not limited to, Bebo, Facebook, LinkedIn, Twitter,