Enviro Electronics Ltd Security Policy

Server Security

The servers at Enviro Electronics Ltd provide a wide variety of services to internal and external users, and many servers also store or process sensitive information for Enviro Electronics Ltd. These hardware devices are vulnerable to attacks from outside sources which require due diligence by the IT Department to secure the hardware against such attacks.

Purpose

The purpose of this policy is to define standards and restrictions for the base configuration of internal server equipment owned and/or operated by or on Enviro Electronics Ltd's internal network(s) or related technology resources via any means. This can include, but is not limited to, the following:

- Internet servers (FTP servers, Web servers, Mail servers, Proxy servers, etc.)
- Application servers
- Database servers
- File servers
- Print servers
- Third-party appliances that manage network resources
- Eliminate configuration errors and reduce workstation outages
- Reduce undocumented workstation configuration changes that tend to open up security vulnerabilities
- Facilitate compliance and demonstrate that the controls are working
- Protect Enviro Electronics Ltd data, networks, and databases from unauthorized use and/or malicious attack

Server Security

Responsibilities

Enviro Electronics Ltd IT Manager has the overall responsibility for the confidentiality, integrity, and availability of Enviro Electronics Ltd data.

Other IT staff members, under the direction of the IT manager, are responsible for following the procedures and policies within IT.

Supported Technology

All servers will be centrally managed by Enviro Electronics Ltd IT Department and will utilize approved server configuration standards. Approved server configuration standards will be established and maintained by Enviro Electronics Ltd IT Department.

All established standards and guidelines for the Enviro Electronics Ltd IT environment are documented in an IT storage location.

- The following outlines Enviro Electronics Ltd minimum system requirements for server equipment supporting Enviro Electronics Ltd systems.
- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the IT Manager.
- Access to services must be logged or protected though appropriate access control methods.
- Security patches must be installed on the system as soon as possible through
- Enviro Electronics Ltd configuration management processes.

Workstation Configuration

Responsibilities

Enviro Electronics Ltd IT Manager has the overall responsibility for the confidentiality, integrity, and availability of Enviro Electronics Ltd data.

Other IT staff members, under the direction of the IT Manager, are responsible for following the procedures and policies within IT.

Supported Technology /R

All workstations will be centrally managed by Enviro Electronics Ltd's IT Department and will utilize approved workstation configuration standards, which will be established and maintained by Enviro Electronics Ltd's IT Department.

All established standards and guidelines for the Enviro Electronics Ltd IT environment are documented in an IT storage location.

The following outlines Enviro Electronics Ltd's minimum system requirements for workstation equipment.

- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the IT Manager.
- All patch management to workstations will be monitored through reporting with effective remediation procedures. Enviro Electronics Ltd has deployed a patch management process; reference the Patch Management Policy.
- All workstations joined to the Enviro Electronics Ltd domain will automatically receive a policy update configuring the workstation to obtain future updates from our desktop management system.

SECURITY POLICY

- All systems within Enviro Electronics Ltd are required to utilize anti-virus, malware, and data leakage protection. IT will obtain alerts of infected workstations and perform certain remediation tasks.
- All workstations will utilize the Enviro Electronics Ltd domain so that all general policies, controls, and monitoring features are enabled for each workstation. No system should be managed manually but should be managed through some central tool or model in order to efficiently manage and maintain system security policies and controls.
- Third-party applications need to be updated and maintained. So that software with security updates is not exposed to vulnerabilities for longer than necessary, a quarterly review will be performed.
- Third-party applications, including browsers, shall be updated and maintained in accordance with the Enviro Electronics Ltd patch management program.
- Any critical security updates for all applications and operating systems need to be reviewed and appropriate actions taken by the IT Department to guarantee the security of the workstations in accordance with the Enviro Electronics Ltd patch management program.
- Internet browsers on workstations will remain up to date. To ensure all browsers are up to date, the IT Department will perform quarterly reviews. If there is a reason the browser cannot be updated, due to conflicts with applications, these exceptions will be recorded.
- By default, all workstations joined to the Enviro Electronics Ltd domain will obtain local security settings through policies.

System Monitoring and Auditing

System monitoring and auditing is used to determine if inappropriate actions have occurred within an information system. System monitoring is used to look for these actions in real time while system auditing looks for them after the fact.

This policy applies to all information systems and information system components of Enviro Electronics Ltd. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities
- Devices that provide centralized storage capabilities
- Desktops, laptops, and other devices that provide distributed computing capabilities
- Routers, switches, and other devices that provide network capabilities
- Firewall, Intrusion Detection/Prevention (IDP) sensors, and other devices that provide dedicated security capabilities

Information systems will be configured to record login/logout and all administrator activities into a log file. Additionally, information systems will be configured to notify administrative personnel if inappropriate, unusual, and/or suspicious activity is noted. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to the IT manager.

Information systems are to be provided with sufficient primary (on-line) storage to retain 30-days' worth of log data and sufficient secondary (off-line) storage to retain one year's worth of data. If primary storage capacity is exceeded, the information system will be configured to overwrite the oldest

logs. In the event of other logging system failures, the information system will be configured to notify an administrator.

System logs shall be manually reviewed weekly. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to appropriate security management personnel.

System logs are considered confidential information. As such, all access to system logs and other system audit information requires prior authorization and strict authentication. Further, access to logs or other system audit information will be captured in the logs.

Physical Access control

This policy applies to all facilities of Enviro Electronics Ltd, within which information systems or information system components are housed. Specifically, it includes:

- Data centers or other facilities for which the primary purpose is the housing of IT infrastructure
- Data rooms or other facilities, within shared purpose facilities, for which one of the primary purposes is the housing of IT infrastructure
- Switch and wiring closets or other facilities, for which the primary purpose is not the housing of IT infrastructure

Access to facilities, information systems, and information system display mechanisms will be limited to authorized personnel only. Authorization will be demonstrated with authorization credentials (badges, identity cards, etc.) that have been issued by Enviro Electronics Ltd.

SECURITY POLICY

Access to facilities will be controlled at defined access points with the use of card readers and locked doors. Before physical access to facilities, information systems, or information system display mechanisms is allowed, authorized personnel are required to authenticate themselves at these access points. The delivery and removal of information systems will also be controlled at these access points. No equipment will be allowed to enter or leave the facility, without prior authorization, and all deliveries and removals will be logged.

A list of authorized personnel will be established and maintained so that newly authorized personnel are immediately appended to the list and those personnel who have lost authorization are immediately removed from the list. This list shall be reviewed and, where necessary, updated on at least an annual basis.

If visitors need access to the facilities that house information systems or to the information systems themselves, those visitors must have prior authorization, must be positively identified, and must have their authorization verified before physical access is granted. Once access has been granted, visitors must be escorted, and their activities monitored at all times.

This policy is complementary to any previously implemented policies dealing specifically with security and network access to Enviro Electronics Ltd's network.

It is the responsibility of each employee of Enviro Electronics Ltd to protect Enviro Electronics Ltd's technology based resources from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to Enviro Electronics Ltd's public image. Procedures will be followed to ensure resources are protected.

- Trust relationships allow users and computers to be authenticated (to have their identity verified) by an authentication authority. Trust relationships should be evaluated for their inherent security risk before implementation.
- Authorized users must always use the standard security principle of "Least Required Access" to perform a function.
- System administration and other privileged access must be performed through a secure connection. Root is a user account that has administrative
- privileges which allows access to any file or folder on the system. Do not use the root account when a non-privileged account will do.
- All Enviro Electronics Ltd servers are to be in access-controlled environments.
- All employees are specifically prohibited from operating servers in environments with uncontrolled access (i.e. offices).

Password Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Enviro Electronics Ltd entire network. As such, all Enviro Electronics Ltd employees or volunteers/directors (including contractors and vendors with access to Enviro Electronics Ltd systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

SECURITY POLICY

This policy applies to all personnel or volunteers/directors who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system that resides at any Enviro Electronics Ltd facility, has access to the Enviro Electronics Ltd network, or stores any non-public Enviro Electronics Ltd information.

User Network Passwords

- Passwords for Enviro Electronics Ltd network access must be implemented according to the following guidelines:
- Passwords must be changed every 90 days
- Passwords must adhere to a minimum length of 10 characters
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#$%^&*_+=?/~';',<>|\).
- Passwords must not be easily tied back to the account owner such as:
- username, social security number, nickname, relative's names, birth date, etc.
- Passwords must not be dictionary words or acronyms
- Passwords cannot be reused for 1 year

System-Level Passwords

- All system-level passwords must adhere to the following guidelines:
- Passwords must be changed at least every 6 months
- All administrator accounts must have 12 character passwords which must contain three of the four items: upper case, lower case, numbers, and special characters.
- Non-expiring passwords must be documented listing the requirements for those accounts. These accounts need to adhere to the same standards as administrator accounts.

- Administrators must not circumvent the Password Policy for the sake of ease of use

Member information

Member information: Any record maintained by, or on behalf of, Enviro Electronics Ltd that contains information regarding an individual who has an established, ongoing relationship with Enviro Electronics Ltd. This includes records, data, files, or other information in paper, electronic, or other form that are maintained by, or on behalf of, any service provider on behalf of Enviro Electronics Ltd.

Member information system: Any electronic or physical method used to access, collect, store, use, transmit, protect, or dispose of member information.

This policy addresses the following topics:

- Board Involvement
- Risk Assessment
- Management and Control of Risk
- Member Information Security Controls
    - Vendor Management Review Program
    - Software Inventory
    - Hardware Inventory
    - Critical Systems List
    - Records Management
    - Clean Desk Policy
    - Hardware and Electronic Media Disposal Policy
    - IT Acquisition Policy
    - Incident Response Plan
    - Information Sharing

- Training
- Testing

Purpose

The purpose of this policy is to ensure that Enviro Electronics Ltd complies with existing UK laws, and to ensure that information regarding members is kept secure and confidential.

Policy Detail

It is the policy of Enviro Electronics Ltd to protect the confidentiality, security, and integrity of each member's non-public personal information in accordance with existing UK laws. Enviro Electronics Ltd will establish and maintain appropriate standards relating to administrative, technical, and physical safeguards for member records and information.

Enviro Electronics Ltd will maintain physical, electronic, and procedural safeguards, which comply with UK Law, to guard members' non-public personal information.

Enviro Electronics Ltd will not gather, collect, or maintain any information about its members that is not necessary to offer its products and services, to complete member transactions, or for other relevant business purposes.

Enviro Electronics Ltd does not sell or provide any member information to third parties, including list services, telemarketing firms, or outside companies for independent use.

Enviro Electronics Ltd Information Manager is responsible for annually reviewing the program, making any needed adjustments, and coordinating staff training. Enviro Electronics Ltd Management is responsible for ensuring that its departments comply with the requirements of the program.

Information Security Program

Management is responsible for developing, implementing, and maintaining an effective information security program to:

- Ensure the security and confidentiality of member records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to, or use of, such records or information that would result in substantial harm or inconvenience to any member

Management shall report to the Directors, at least annually, on the current status of Enviro Electronics Ltd's Information Security Program. The Board of Directors will also be notified of any security breaches or violations and the management team's response and recommendations for changes in the Information Security Program

Risk Assessment

Enviro Electronics Ltd maintains a risk assessment that identifies potential threats to member information and evaluates the potential impact of the threats.

On an annual basis, the risk assessment is reviewed and updated by the IT Manager and Enviro Electronics Ltd Management. Enviro Electronics Ltd controls are then updated accordingly.

Management and Control of Risk

In order to manage and control the risks that have been identified, Enviro Electronics Ltd will:

- Establish written procedures designed to implement, maintain, and enforce
- Enviro Electronics Ltd information security program

- Limit access to Enviro Electronics Ltd member information systems to authorized
- employees only
- Establish controls to prevent employees from providing member information to unauthorized individuals
- Limit access at Enviro Electronics Ltd's physical locations containing member information, such as building, computer facilities, and records storage facilities, to authorized individuals only
- Provide encryption of electronic member information including, but not limited to, information in transit or in storage on networks or systems to which unauthorized individuals may have access.
- Ensure that member information system modifications are consistent with
- Enviro Electronics Ltd's information security program
- Implement dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, member information
- Monitor Enviro Electronics Ltd's systems and procedures to detect actual and attempted
- attacks on, or intrusions into, the member information systems
- Establish response programs that specify actions to be taken when Enviro Electronics Ltd suspects or detects that unauthorized individuals

have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies

- Implement measures to protect against destruction, loss, or damage of member information due to environmental hazards, such as fire and water damage or technical failures
- Regularly test, monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in

technology, the sensitivity of member information, business arrangements, outsourcing arrangements, and internal or external threats to Enviro Electronics Ltd's information security systems

Member information security controls /R

Enviro Electronics Ltd has established a series of member information security controls to manage the threats identified in the risk assessment. The controls fall into ten categories.

- **Vendor management review program**
  Enviro Electronics Ltd will exercise appropriate due diligence when selecting service providers. When conducting due diligence, management will conduct a documented vendor review process as outlined in the Vendor Due Diligence Procedure.
  All service providers, who may access member information, must complete a Vendor Confidentiality Agreement requiring the provider to maintain the safekeeping and confidentiality of member information in compliance with applicable UK laws. Such agreements must be obtained prior to any sharing of member information. Once the agreement has been completed, management will, according to risk, monitor service providers by reviewing audits, summaries of test results, or other evaluations.

- **Software inventory**
  Enviro Electronics Ltd will maintain an inventory of its desktop, server, and infrastructure software. The information from this collection will provide critical information in identifying the software required for rebuilding systems. A template incorporated into the software inventory ensures that the security configuration and configuration standards are enforced. The template will also provide personnel with

a quick resource in the event of a disaster. The software inventory list will be reviewed and updated on a continual basis.

- **Hardware inventory**
  Enviro Electronics Ltd will maintain an inventory of its desktop, server, and infrastructure hardware. The information from this collection will provide critical information in identifying the hardware requirements for rebuilding systems. A template incorporated into the hardware inventory ensures that Enviro Electronics Ltd standards are enforced. The template will also provide personnel with a quick resource in the event of a disaster. The hardware inventory list will be reviewed and updated on a continual basis.
- **Critical systems list**
  Enviro Electronics Ltd will maintain a listing of its critical systems. This listing will support critical reliability functions, communications, services, and data. The identification of these systems is crucial for securing member information from vulnerabilities, performing impact analysis, and in preparing for unscheduled events that affect the operations of Enviro Electronics Ltd.
- **Records management**
  The industry wide general principles of records management apply to records in any format. Enviro Electronics Ltd will adhere to policies and procedures for protecting critical records from all outside and unauthorized access. Access to sensitive data will be defined as to who can access which data and under what circumstances. The access will be logged to provide accountability.
  Enviro Electronics Ltd will adhere to the required Data Classification Procedures, and designated for record retention. Enviro Electronics Ltd will adhere to the Records Retention Policy for the proper process to dispose of records. Record disposal will be well documented. An inventory will be maintained of

the types of records that are disposed of, including certification that the records have been destroyed.

- **Clean desk policy**
  Enviro Electronics Ltd employees will comply with the Clean Desk Policy. This policy was developed to protect sensitive data from being readily available to unauthorized individuals.
- **Hardware and electronic media disposal procedure**
  Enviro Electronics Ltd will take precautions, as outlined in the Hardware and Electronic Media Disposal Policy, to ensure sensitive data cannot be retrieved from retired hardware or electronic media.
- **IT acquisition policy**
  Enviro Electronics Ltd will adhere to policies and procedures for acquisition of computer related items. Computer related purchases will be reviewed by designated IT personnel for compliance with security plans and alignment with operational and strategic plans. An annual review of acquisition policies and procedures will occur with input from the IT Manager.
  A review of technology needs will occur during the annual budgeting and work planning processes. Needs will be classified into either current year plans or long range needs. The acquisition of technology solutions will be assessed to ensure that both current and future needs are met.
- **Incident response plan /R**
  Incident response is defined as an organized approach to addressing and managing the aftermath of a security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.
  As required in the Incident Response Plan, Enviro Electronics Ltd will assemble a team to handle any incidents that occur. Necessary actions to prepare Enviro Electronics Ltd and the Incident Response Team will be

conducted prior to an incident as required in the Incident Response Plan.

Below is a summary of the steps the IT Department, as well as Enviro Electronics Ltd management, would take:

- The IT Department will immediately investigate the intrusion to:
  - Prevent any further intrusion to the system
  - Determine the extent of the intrusion and any damage caused
  - Take any steps possible to prevent any future such intrusions
- The IT Department will notify Administrative Management and Risk Management of the intrusion. Administrative Management will be responsible for notifying the Board of Directors.
- The IT Department will follow escalation processes and notification procedures as outlined in the Incident Response Plan. Examples include, but are not limited to, notifications to staff, regulatory agencies, law enforcement agencies or the public.

Training

Enviro Electronics Ltd recognizes that adequate training is of primary importance in preventing IT security breaches, virus outbreaks, and other related problems. Enviro Electronics Ltd will conduct regular IT training through methods such as staff meetings and computer based tutorial programs. In addition, employees will be trained to recognize, respond to, and where appropriate, report any unauthorized or fraudulent attempts to obtain member information.

All new employees will receive IT Security Training, as part of their orientation training, emphasizing security and IT responsibility. The Training Specialist, or designee, is responsible for training new employees on Information Security.

Testing

The IT Manager annually audits Enviro Electronics Ltd's Safeguarding Member Information Program. The IT Manager provides a formal report of its findings to Senior Management, the Security Officer, and the Board of Directors.

Enviro Electronics Ltd will require periodic tests of the key controls, systems, and procedures of the information security program. In accordance with current industry standards, the frequency and nature of such tests shall be determined by the IT Department.

The IT Manager will be responsible for reviewing the results of these tests and for making recommendations for improvements where needed.

Security Incident Management Policy

Security Incident Management at Enviro Electronics Ltd is necessary to detect security incidents, determine the magnitude of the threat presented by these incidents, respond to these incidents, and if required, notify Enviro Electronics Ltd members of the breach.

Program Organization

- **Computer Emergency Response Plans** - Enviro Electronics Ltd management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or degradation of service. For example, Charter connectivity is interrupted or an isolated malware discovery.
- **Incident Response Plan Contents** - The Enviro Electronics Ltd incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise, including notification of relevant external partners. Specific areas covered in the plan include:
    - Specific incident response procedures

- Business recovery and continuity procedures
- Data backup processes
- Analysis of legal requirements for reporting compromises
- Identification and coverage for all critical system components
- Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers

- **Incident Response Testing** - at least once every year, the IT Department must utilize simulated incidents to mobilize and test the adequacy of response. Where appropriate, tests will be integrated with testing of related plans (Business Continuity Plan, Disaster Recovery Plan, etc.) where such plans exist. The results of these tests will be documented and shared with key stakeholders.
- **Incident Response and Recovery** - A security incident response capability will be developed and implemented for all information systems that house or access Enviro Electronics Ltd controlled information. The incident response capability will include a defined plan and will address the seven stages of incident response:
    - Preparation
    - Detection
    - Analysis
    - Containment
    - Eradication
    - Recovery
    - Post-Incident Activity
    - To facilitate incident response operations, responsibility for incident handling operations will be assigned to an incident response team. If an incident occurs, the members of this team will be charged with executing the incident response plan. To ensure that the team is fully prepared for its responsibilities, all team members will be trained in incident response operations on an annual basis.

- Incident response plans will be reviewed and, where applicable, revised on an annual basis. The reviews will be based upon the documented results of previously conducted tests or live executions of the incident response plan. Upon completion of plan revision, updated plans will be distributed to key stakeholder

- **Intrusion Response Procedures** - The IT Department must document and periodically revise the Incident Response Plan with intrusion response procedures. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.
- **Malicious Code Remediation** - Steps followed will vary based on scope and severity of a malicious code incident as determined by Information Security Management. They may include but are not limited to: malware removal with one or more tools, data quarantine, permanent data deletion, hard drive wiping, or hard drive/media destruction.
- **Data Breach Management** - Enviro Electronics Ltd management should prepare, test, and annually update the Incident Response Plan that addresses policies and procedures for responding in the event of a breach of sensitive customer data.
- **Incident Response Plan Evolution** - The Incident Response Plan must be updated to reflect the lessons learned from actual incidents. The Incident Response Plan must be updated to reflect developments in the industry.

Program Communication

- **Reporting to Third Parties** - Unless required by law or regulation to report information security violations to external authorities, senior management, in conjunction with legal representatives, the Security Officer, and the IT Manager of IT must weigh the pros and cons of external disclosure before reporting these violations.
    - If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.
    - If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Security Officer must be notified immediately.
- **Display of Incident Reporting Contact Information** - Enviro Electronics Ltd contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters, and the intranet.
- Member Notification - The notification will be conducted and overseen by Enviro Electronics Ltd's Director of Risk Management. The notification should contain, at a minimum, the following elements:
    - Recommendations for the member to protect him/herself
    - Contact information for the credit bureaus

Hardware and Media Disposal

Purpose

Enviro Electronics Ltd owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse, including media, are covered by this policy.

Where assets have not reached end of life, it is desirable to take advantage of residual value through reselling, auctioning, donating, or reassignment to a less critical function. This policy will establish and define standards, procedures, and restrictions for the disposition of non-leased IT equipment and media in a legal, cost-effective manner.

Enviro Electronics Ltd's surplus or obsolete IT assets and resources (i.e. desktop computers, servers, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and Enviro Electronics Ltd's upgrade guidelines.

All disposition procedures for retired IT assets must adhere to company approved methods.

Policy Detail

coordinated by Enviro Electronics Ltd's IT Department. The IT Department is responsible for backing up data from IT assets slated for disposition (if applicable) and removing company tags and/or identifying labels. IT is responsible for selecting and approving external agents for hardware sanitization, reselling, recycling, or destruction of the equipment. IT is also responsible for the chain of custody in acquiring credible documentation from contracted third parties that verify adequate disposition and disposal that adhere to legal requirements and environmental regulations.

It is the responsibility of any employee of Enviro Electronics Ltd's IT Department, with the appropriate authority, to ensure that IT assets are disposed of according to the methods in the Hardware and Electronic Media Disposal Procedure. It is imperative that all dispositions are done appropriately, responsibly, and according to IT lifecycle standards, as well as with Enviro Electronics Ltd's resource planning in mind. Hardware asset types and electronic media that require secure disposal include, but are not limited to, the following:

- Computers (desktops and laptops)

- Printers
- Handheld devices
- Servers
- Networking devices (hubs, switches, bridges, and routers)
- Floppy disks
- Backup tapes
- CDs and DVDs
- Zip drives
- Hard drives / Flash memory
- Other portable storage device

Anti Virus

Malware threats must be managed to minimize the amount of downtime realized by Enviro Electronics Ltd's systems and prevent risk to critical systems and member data. This policy is established to:

- Create prudent and acceptable practices regarding anti-virus management
- Define key terms regarding malware and anti-virus protection
- Educate individuals, who utilize Enviro Electronics Ltd system resources, on the responsibilities associated with anti-virus protection

Note: The terms virus and malware, as well as anti-virus and anti-malware, may be used interchangeably.

Purpose

This policy was established to help prevent infection of Enviro Electronics Ltd computers, networks, and technology systems from malware and other malicious code. This policy is intended to help prevent damage to user applications, data, files, and hardware.

This policy applies to all computers connecting to the Enviro Electronics Ltd network for communications, file sharing, etc. This includes, but is not limited to, desktop computers, laptop computers, servers, and any PC based equipment connecting to the Enviro Electronics Ltd network.

Policy Detail

All computer devices connected to the Enviro Electronics Ltd network and networked resources shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices.

The virus protection software must not be disabled or bypassed without IT approval.

The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

Each file server, attached to the Enviro Electronics Ltd network, must utilize Enviro Electronics Ltd IT approved virus protection software and setup to detect and clean viruses that may infect Enviro Electronics Ltd resources.

Each e-mail gateway must utilize Enviro Electronics Ltd IT approved e-mail virus protection software.

All files on computer devices will be scanned periodically for malware.

Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Service Desk.

If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device

may be disconnected from the Enviro Electronics Ltd network until the infection has been removed.

Users should:

- Avoid viruses by never opening any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately then remove them from the Trash or Recycle Bin.
- Delete spam, chain, or other junk mail without opening or forwarding the item.
- Never download files from unknown or suspicious sources.
- Always scan removable media from an unknown or non-Enviro Electronics Ltd source (such as a CD or USB from a vendor) for viruses before using it.
- Back up critical data on a regular basis and store the data in a safe place. Critical Enviro Electronics Ltd data can be saved to network drives and are backed up on a periodic basis. Contact the Enviro Electronics Ltd IT Department for details.

Because new viruses are discovered every day, users should periodically check the Anti-Virus Policy for updates. The Enviro Electronics Ltd IT Department should be contacted for updated recommendations.

Account Management

Computer accounts are the means used to grant access to Enviro Electronics Ltd's information systems. These accounts provide a means of providing accountability, a key to any computer security program, for Enviro Electronics Ltd usage.

This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Purpose

The purpose of this policy is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at Enviro Electronics Ltd.

This policy applies to the employees, Directors, volunteers, contractors, consultants, temporaries, and other workers at Enviro Electronics Ltd, including all personnel affiliated with third parties with authorized access to any Enviro Electronics Ltd information system.

Policy Detail

Accounts

- All accounts created must have an associated written request and signed management approval that is appropriate for the Enviro Electronics Ltd system or service.
- All accounts must be uniquely identifiable using the assigned username.
- Shared accounts on Enviro Electronics Ltd information systems are not permitted.
- Reference the Employee Access During Leave of Absence Policy for removing an employee's access while on a leave of absence or vacation.
- All default passwords for accounts must be constructed in accordance with the Enviro Electronics Ltd Password Policy.
- All accounts must have a password expiration that complies with the Enviro Electronics Ltd Password Policy.
- Concurrent connections may be limited for technical or security reasons.
- All accounts must be disabled immediately upon notification of any employee's termination.

Account Management

SECURITY POLICY

The following items apply to System Administrators or designated staff:

- Information system user accounts are to be constructed so that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with an individual's account. Further, to eliminate conflicts of interest, accounts shall be created so that no one user can authorize, perform, review, and audit a single transaction.
- All information system accounts will be actively managed. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
- Access controls will be determined by following established procedures for new employees, employee changes, employee terminations, and leave of absence.
- All account modifications must have a documented process to modify a user account to accommodate situations such as name changes and permission changes.
- Information system accounts are to be reviewed monthly to identify inactive accounts. If an employee or third party account is found to be inactive for 30 days, the owners (of the account) and their manager will be notified of pending disablement. If the account continues to remain inactive for 15 days, it will be manually disabled.
- A list of accounts, for the systems they administer, must be provided when requested by authorized Enviro Electronics Ltd management.
- An independent audit review may be performed to ensure the accounts are properly managed.