TRADEWALK BROKING PRIVATE LIMITED

ACCESS CONTROL POLICY

Effective security controls in relation to access to data are an essential component of the effective risk management. Access controls protect information by managing access at all entry and exit points, both logical and physical. These measures ensure that only authorized users have access to specific information, systems and facilities. Therefore, the application of access controls, the management of user accounts and the monitoring of their use plays an extremely important part in the overall security of information resources.

Access controls are established for all major information, information systems and facilities based on their classification and security risk assessment to ensure that the appropriate level of security is implemented.

The company has in place adequate controls for access to server rooms by restricting entry except the directors and compliance officer and proper audit trails are maintained for all unauthorized entry and exit of people for the same.

1. Access to information are controlled based on business and security requirements and the access control rules

a. Both logical and physical access controls.

b. An identified business requirement for the user to have access to the information or process (both 'need-to-know' and 'need-to-use' principles).

c. All access is denied unless specifically approved under the provisions of this policy

d. Changes in user permission whether performed automatically or by an administrator

e. The terms and conditions for access provided

2. Access to networks and network services are authorized and controlled based on business, security requirements and access control rules defined for each network. These rules are take include the followings:

a. Security requirements of the network or network services.

b. An identified business requirement for the user to have access to the network (e.g., use of VPN or wireless network) or network services ('need-to-have' principle).

c. The user's security classification and the security classification of the network.

d. The user's authentication requirements for accessing various network services.

e. Monitoring and managing of the use of network services.

f. The authorization mechanisms for determining who is allowed to access which networks and network services.

g. Security policies of operating system.

h. Updated antivirus definitions.

i. Firewall security rules

3. **Access to shared folders are consider the followings:**

a. Only authorized for specific employees.

b. Sharing any non-related business materials (e.g., photos, videos, audio files, etc.) shall not be permitted.

4. **User Registration and De-Registration**

a. There a formal access control procedure that includes clear steps in relation to requesting, creating, modifying, suspending and revoking user accounts.

5. **The granting of user access, changes to existing user access rights and removal of user access is authorized by Owner taking into account the following**

a. Least privilege (‘need-to-know’ principle).

b. Segregation of duties.

c. Level of access required.

6. **Use of Secret Authentication Information**

a. Users shall be accountable for any activity associated with their access rights.

b. Users shall not capture or otherwise obtain passwords, decryption keys or any other secret authentication method that could permit unauthorized access.

7. **Users can’t do the following:**

a. Reveal a password over the phone to anyone.

b. Reveal a password in an email message.

c. Reveal or distribute a password to others even to Administrators or his boss.

d. Talk about a password in front of other.

e. Hint at the format of a password: ▪ Name of family, friends and co-workers ▪ Birthday, address and phone number ▪ Patterns: “aaabbb” and “1112222”

f. Reveal a password on questionnaires or security forms.

g. Share a password with family members. .

h. Reveal a password to co-workers while on vacation.

i. Write a password on a piece of paper and left in a place where unauthorized users are able to discover them

BUSINESS CONTINUITY PLANING AND DESASTER RECOVERY POLICY

The Company is in the business of share and stock business and. The entire business module is the function of proper human resource utilization / management and the state of art of technology / I.T. infrastructure amongst others.

Our business continuity plan takes on to consideration the following action plan:
1. **Recovery, resumption and maintenance** of all aspects including human resource and technology.
2. Prioritization of **business objectives Regular updates to the BCP**.
3. A cyclical process oriented approach with **proper risk assessment, implementation and management**. The above points are detailed hereunder:-

1. **Recovery, resumption and maintenance**
Share and trading business is the key activities to the organization. In order to this business the company has implemented various CTCL, software's in addition to NEAT System for trading with NSE and /Respective vendors make constant up gradations and implementation accordingly. Trained human resources are employed for the purpose.

A detailed policy for disaster recovery is separately made and successfully implemented in the organization, which includes DRP, changes Management amongst others.

a) Data Recovery
A proper Data Backup policy stating the recovery, resumption and restoration of the data is adapted and following by the company. The company ensures the restoration of data at intervals to ensure business continuity in time of crisis.

b) System & Hardware's
The Company claim to have a techno-savy environment. As management policy it keeps on investing in upgraded hardware's and software's are required from time to time.

c) Monetary Loss
Increasing complexities in the financial business environment attracts new risk to the business model. The company always looks forward for implementation of new software's to counter such monetary losses.

d) Environmental

Flood, Earthquakes, Riot, Fire etc are the threats for which the company has continuity plans.
- Long Term Plans
    - ➢ Offsite operations
- Continuous Plans
    - ➢ Insurance Policies
    - ➢ Maintenance of server / software's.
    - ➢ Backup

e) Recovery Plans

The biggest challenge is the recovery of the business in times of crisis. The crisis may come for the following factors:

➢ Data Backup – Please refer to backup policy.
➢ Server- Maintenance contracts are given.
➢ Nodes – Front and user – An in house efficient team is there to look after
➢ Software's – Front and back –Appropriate contracts are made with the vendors to ensure smooth functioning.

2. Business Objectives

Prioritization of financial services to the best of satisfaction of its clients and realization of own set targets are the prime objectives of the company.

In the existing dynamic market situation the company need to constantly vouch for the latest development in the market environment with regards to available models of business and the requisite I.T and human resources.

Accordingly the company has evolutes its paradigm from the conventional self centered business to break into retail segment. Similarly on the I.T front various new software's have been introduced onto the system.

3. Regular Updates to the BCP

The company has a technology savy senior management team who understand the entire prospects of the business viz-a-viz technological changes, understanding the critical operation, business dynamics, human resources management, general administration and all other related matters.

The said senior management team constantly interacts on the evolution if the BCP.

4. Proper Risk assessment, implementation and management

Assessing and managing the risk is the key function of the business. Any miss-assessment of the risk for transaction done whether for transaction done whether for self or for clients may have adverse impact on the company business. Therefore, the proper risk assessment for all the processes is very important. The business models are accordingly formulated.

Once the models are formulated proper implementation and management of the same is done with available I.T. human resource in light of the relevant policies of the company formulated for the purpose

Data Backup Policy

Best Practice:

A backup policy helps manage users' expectations and provides specific guidance on the "who, what, when, and how" of the data backup and restore process. There are several benefits to documenting your data backup policy:

- Helps clarify the policies, procedures, and responsibilities

- Allows you to dictate:

- Where backups are located

- Who can access backups and how they can be contacted

- How often data should be backed up

- What kind of backups are performed and

- What hardware and software are recommended for performing backups

- Identifies any other policies or procedures that may already exist (such as contingency plans) or which ones may supersede the policy

- Has a well-defined schedule for performing backups

- Identifies who is responsible for performing the backups and their contact information. This should include more than one person, in case the primary person responsible is unavailable

- Identifies who is responsible for checking the backups have been performed successfully, how and when they will perform this

- Ensures data can be completely restored

- Has training for those responsible for performing the backups and for the users who may need to access the backups

- Is partially, if not fully automated

- Ensures that more than one copy of the backup exists and that it is not located in same location as the originating data

- Ensures that a variety of media are used to backup data, as each media type has its own inherent reliability issues

- Ensures the structure of the data being backed up mirrors the originating data

- Notes whether or not the data will be archived

If this information is located in one place, it makes it easier for anyone needing the information to access it. In addition, if a backup policy is in place, anyone new to the project or office can be given the documentation which will help inform them and provide guidance.

Description Rationale:

Collecting information about backing data up before it is needed helps prevent problems and delays that may be encountered when a user needs data from a backup.

Data Retention and Disposal Policy

1. Policy Information

Organization: Tradewalk Broking Private Limited.
Policy Approved by: Mr. Udit Aggarwal-Director

2. Introduction

a. Purpose of the policy:

- The purpose of this Policy is to ensure that necessary records and documents of are adequately protected and maintained and to ensure that records that are no longer needed by Tradewalk Broking Private Limited or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees of Tradewalk Broking Private Limited in understanding their obligations in retaining electronic documents - including email, text files, digital images, sound and movie files, PDF documents, and all Microsoft Office or other formatted files or paper documents.

b. Policy Statement:

- This Policy represents Tradewalk Broking Private Limited regarding the retention and disposal of records and the retention and disposal of electronic documents.

3. Scope

This policy applies to employees, staff, and other personnel who are responsible for owning and managing records and documents in either paper or electronic formats.

4. Policy

This policy defines the Data retention and destruction schedule for paper and electronic records. The Data Retention Schedule is approved as the initial maintenance, retention and disposal schedule for the physical (paper) and electronic records of Tradewalk Broking Private Limited. The IT committee of Cyber is responsible for the administration of this policy and the implementation of processes and procedures. In conjunction with General Counsel, the Administrator is also authorized to; make

modifications to the Record Retention Schedule as needed to ensure that it is in compliance with state and federal laws; ensure the appropriate categorization of documents and records on behalf of the company annually review the policy; and monitor compliance with this policy.

5. Responsibilities of Staff

All staff is responsible for:

• checking that any information that they provide to the Administration in regards to their employment is accurate and up to date.
• informing the Administration of any changes to information, which they have provided i.e. changes of address
• Checking the information that the Organization will send out from time to time, giving details of information kept and processed about staff.
• Informing Tradewalk Broking Private Limited (Compliance Officer) of any errors or changes. The Academy cannot be held responsible for any errors unless the staff member has informed the management of them.

6. Data Security

a. All staff are responsible for ensuring that: Any personal data which they hold is kept securely. Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

b. Staff should note that unauthorised disclosure and/or failure to adhere to the requirements set out above will usually be a disciplinary matter, and may be considered gross misconduct in some Data cases.

c. Personal information should be; kept in a locked filing cabinet; or in a locked drawer; or if it is computerised, be password protected; or when kept or in transit on portable media the files themselves must be password protected.

d. Personal data should never be stored at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites,

e. Ordinarily, personal data should not be processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Data Controller must be obtained, and all the security guidelines given in this document must still be followed.

f. Data stored on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment.

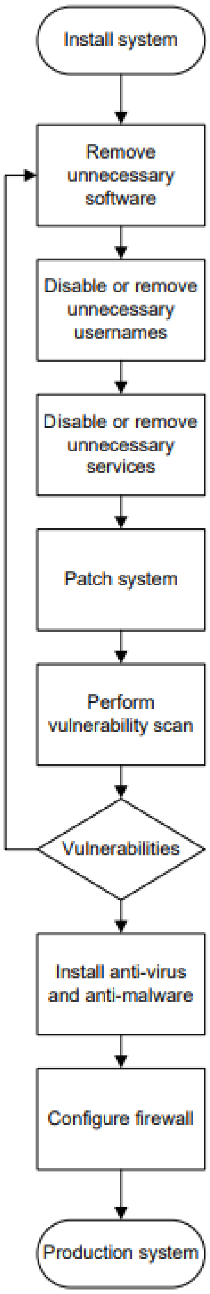
Data Retention Guidelines

Records

a. Articles of Incorporation and amendments	Permanently
b. Policies	Permanently
c. Meeting Minutes	Permanently
d. SEBI Registration Certificate	Permanently
e. Correspondence relating to Exchange	Permanently
f. Correspondence relating to Clients	Till Trading Account Active and after closure 10 years
g. Compliances Report	Permanently

System /Network Hardening Policy

The organizations   is hardened according to this policy to minimize Tradewalk lnerabilities and process is given in diagram.


Install system
Remove unnecessary software
Disable or remove unnecessary usernames
Disable or remove unnecessary services
Patch system
Perform vulnerability scan
Vulnerabilities
Install anti-virus and anti-malware
Configure firewall
Production system

A. Process

1. Install System

2. Install the systems as per the vendor’s instructions.

3. Remove Unnecessary Software

4. Most some systems come with a variety of software packages to provide functionality to all users. Software that that is not going to be used in a particular installation should be removed or uninstalled from the system.

5. Disable or Remove Unnecessary Usernames

6. Most systems come with a set of predefined user accounts. These accounts are provided to enable a variety of functions. Accounts relating to services or functions which are not used should be removed or disabled. For all accounts which are used the default passwords should be changed. Consideration should be given to renaming predefined accounts if it will not adversely affect the system.

7. Disable or Remove Unnecessary Services.

8. All services which are not going to be used in production should be disabled or removed.

9. Patch System

10. The system should be patched up to date. All relevant service packs and security patches should be applied.

11. Perform Tradewalklnerability Scan

12. The system should be scanned with a suitable Tradewalklnerability scanner. The results of the scan should be reviewed and any issues identified should be resolved.

13. Tradewalklnerabilities

14. If there are no significant Tradewalklnerabilities the system can be prepared for live use.

15. Install Anti-Virus and Anti-Malware

16. A suitable anti-virus and anti-malware package should installed on the system to prevent malicious software introducing weaknesses in to the system.

17. Configure Firewall

18. If the system can run its own firewall then suitable rules should be configured on the firewall to close all ports not required for production use.

TRADEWALK
A Journey Towards Success

Incident Management Policy

1. Incident Reporting System

Personnel are required to promptly report possible or known information security and confidentiality violations to IT; including the following:

a. Data incident: any loss, theft, or compromise of information.

b. Infrastructure incident: any event considered to be a malicious action that causes a failure, interruption, or loss in availability to any Information Resource.

c. Unauthorized access incident: any unauthorized access to an information resource

Potential incidents and threats reported from event logging, Tradewalklnerability management, and other monitoring activities must be reported to IT Team
All reported incidents must be assessed by (District/Organization) IT to determine the threat type and activate the appropriate response procedures.

2. Response Team

Incident Response Commander will establish and provide overall direction to an Incident Response Team (IT).
The Incident Response Commander is responsible for overseeing the creation, implementation, and maintenance of an Incident Management Plan.
IT members have pre-defined roles and responsibilities which can take priority over normal duties.
Any additional staff member may be called upon to assist in resolving an incident.

The IT will respond to any new threat to information systems or data following the Incident Management Plan.

The Incident Response Commander must report the incident to

a. Executive Management

b. Any affected User and or/partners

c. Local, state, or federal law officials as required by applicable statutes and/or regulations.

Internet Access Policy

TRADEWALK may provide users/Employee with Internet access to help you do your job. This policy explains our guidelines for using the Internet.

All Internet data that is written, sent, or received through our computer systems is part of official TRADEWALK records. That means that we can be legally required to show that information to law enforcement or other parties. Therefore, you should always make sure that the business information contained in Internet email messages and other transmissions is accurate, appropriate, ethical, and legal.

The equipment, services, and technology that you use to access the Internet are the property of TRADEWALK. Therefore, we reserve the right to monitor how you use the Internet. We also reserve the right to find and read any data that you write, send, or receive through our online connections or is stored in our computer systems.

You may not write, send, read, or receive data through the Internet that contains content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person.

Examples of unacceptable content include (but are not limited to) sexual comments or images, racial slurs, gender-specific comments, or other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

TRADEWALK does not allow the unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet. As a general rule, if you did not create the material, do not own the rights to it, or have not received authorization for its use, you may not put the material on the Internet. You are also responsible for making sure that anyone who sends you material over the Internet has the appropriate distribution rights.

If you use the Internet in a way that violates the law or TRADEWALK. Policies, you will be subject to disciplinary action, up to and including termination of employment. You may also be held personally liable for violating this policy.

The following are examples of prohibited activities that violate this Internet policy:

- Sending or posting discriminatory, harassing, or threatening messages or images
- Using the organization's time and resources for personal gain stealing, using, or disclosing someone else's code or password without authorization copying, pirating, or downloading software and electronic files without permission sending or posting confidential material, trade secrets, or proprietary information outside of the organization violating copyright law failing to observe licensing agreements engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions sending or posting messages or material that could damage the organization's image or reputation.
- Participating in the viewing or exchange of pornography or obscene materials
- Sending or posting messages that defame or slander other individuals
- Attempting to break into the computer system of another organization or person

- Refusing to cooperate with a security investigation
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Using the Internet for political causes or activities, religious activities, or any sort of gambling
- Jeopardizing the security of the organization's electronic communications systems
- Sending or posting messages that disparage another organization's products or services
- Passing off personal views as representing those of the organization
- Sending anonymous email messages
- Engaging in any other illegal activities

Malware management policy

1. Purpose

This document describes the measures taken by the TRADEWALK to counter computer viruses and identifies the responsibilities of individuals. Information security department will be ensuring the security of the TRADEWALK against viruses and other Tradewalk lnerabilities. This policy applies to all devices connected to the Tradewalk's network.

2. Scope

Computing platforms (including but not limited to: desktop workstations, laptops, hand-held, personal digital assistants, servers and network devices) are integral elements in the operations of the TRADEWALK and as such are vital to the TRADEWALK mission. This policy will help ensure that all Tradewalk inerrable computing platforms on premises are guarded against Tradewalk lnerrabilities and protected by antivirus software at all times.

3. Objectives

The principal concern of this computer virus protection policy is effective and efficient prevention of all network virus outbreaks and network security attacks involving all computers associated with TRADEWALK. The primary focus is to ensure that TRADEWALK-affiliated users (Staff) are aware of and take responsibility for the proper use of the TRADEWALK provided and Technology and Network Services-supported virus protection software. This policy is intended to ensure the integrity, reliability, and good performance of TRADEWALK's computing resources; that the resource-user community operates according to a minimum of safe computing practices; that the TRADEWALK's licensed Antivirus virus software is used for its intended purposes; and that appropriate measures are in place to reasonably assure that this policy is honoured.

4. Policy Statement

- Any computer, server or network devices connected to the TRADEWALK's network shall be protected by antivirus software from malicious electronic intrusion.

- All computers or networked devices shall have applicable operating system and application security patches and updates installed prior to initial connection to the network.

- A policy shall be established for prohibiting the use of unauthorized software.

- A formal policy shall be prepared to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken.

- In case of requirement to connect Personal devices to TRADEWALK network, Device shall have antivirus software installed and configured as per the "BYOD policy" for effective operation prior to their connection to the premises network.

- Logs of scan shall be periodically reviewed.

- Reducing Tradewalk lnerabilities that shall prove to be exploited by malware,

- Conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments shall be formally investigated by the TRADEWALK.

- All the files shall be scanned that are received over networks or via any form of storage medium, for malware before use.

- All files shall be scanned, received in form of electronic mail attachments and downloads for malware before use.

- Web pages shall be scanned for malware

PASSWORD POLICY

Security Policy

1. Overview

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 Tradewalk’s entire corporate network As such, all Tradewalk employees or volunteers/directors (including contractors and vendors with access to Tradewalk systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Audience

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 Tradewalk facility, has access to the Tradewalk network, or stores any non-public Tradewalk information.

3. Policy Detail

a. User Network Passwords

Passwords for Tradewalk 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

b. 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

c. Password Protection

The same password must not be used for multiple accounts.
Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Tradewalk information.
Stored passwords must be encrypted.
Passwords must not be inserted in e-mail messages or other forms of electronic communication.
Passwords must not be revealed over the phone to anyone.
Passwords must not be revealed on questionnaires or security forms.

Users must not hint at the format of a password (for example, “my family name”).

Tradewalk passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.

Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.

If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:

Take control of the passwords and protect them

Report the discovery to IT

Users cannot circumvent password entry with an auto logon, application remembering, embedded scripts, or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup processes) with the approval of IT. For an exception to be approved, there must be a procedure to change the passwords.

PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.

If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:

Take control of the passwords and protect them
Report the discovery to IT
Security tokens (i.e. smartcards, RSA hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with Tradewalk.
d. Application Development Standards
a. Application developers must ensure their programs follow security precautions in this policy and industry standards

Patch management policy

1. Introduction

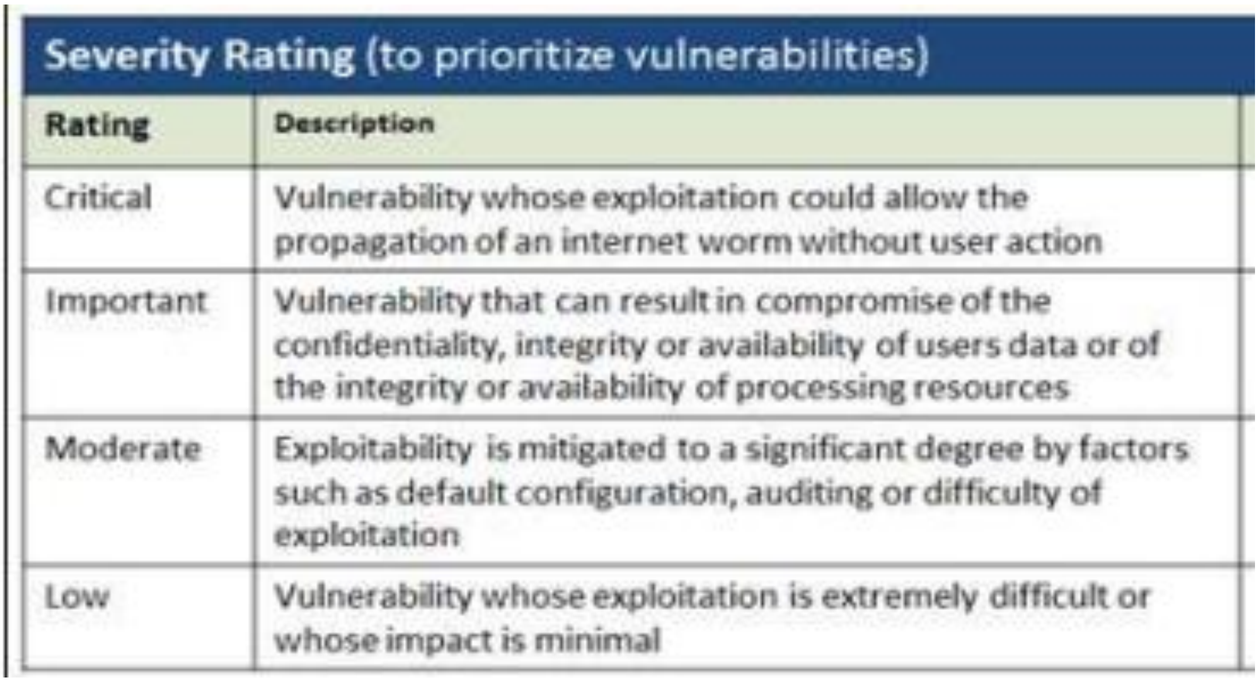
a. This document describes the requirements for maintaining up-to-date systems and software on all IT Systems managed or maintained by the Tradewalk of Tradewalk.

b. The Tradewalk of Tradewalk has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems on and off site which includes systems and services supplied by third parties but managed by the Tradewalk of Tradewalk.

c. The Tradewalk has an obligation to provide appropriate and adequate protection of all its IT estate whether physical, virtual, on premise or in the Cloud.

d. Effective implementation of this policy reduces the likelihood of system compromise due to known vulnerabilities

e. Patches are rated as shown in the tables below.



Severity Rating (to prioritize vulnerabilities)

Rating	Description
Critical	Vulnerability whose exploitation could allow the propagation of an internet worm without user action
Important	Vulnerability that can result in compromise of the confidentiality, integrity or availability of users data or of the integrity or availability of processing resources
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing or difficulty of exploitation
Low	Vulnerability whose exploitation is extremely difficult or whose impact is minimal

2. Scope

a. All IT systems owned by the Tradewalk of Tradewalk and managed by the Tradewalk IT department.

b. All IT systems used by the Tradewalk of Tradewalk but managed by third parties.

3. Responsibilities

a. The Chief Information Officer is accountable for ensuring that the software update and patching policy is adhered to.

b. The IT Services Manager is responsible for ensuring that in scope software is maintained through regular software updates and patching.

c. System owners are responsible for ensuring that all in scope software they manage is maintained through regular software updates and patching.

d. The Tradewalk’s IT department is responsible for ensuring that all in scope software they manage is maintained through regular software updates and patching.

e. The Tradewalk’s IT department is responsible for routinely assessing compliance with the patching policy and will provide guidance to all the stakeholder groups in relation to issues of security and patch management.

f. Third Party Suppliers are responsible for ensuring that all in scope software they manage is maintained through regular software updates and patching, both before and during their operational deployment. Where this is not possible, this must be escalated to the Tradewalk IT

4. Definition

a. System Owners includes Business Systems Managers, Assistant Systems Support Analysts and Business Systems Support Analysts.

b. The Tradewalk’s IT department includes the Core Systems Manager, Solutions Analyst, Deputy Director IT and IT Security Manager.

c. IT Systems refers to: o Physical Servers o Virtual Servers o Cloud hosted Servers o Third Party Managed Servers o End user compute devices (laptops/desktops etc.) o Mobile devices (phones, tablets etc.) o Server Operating Systems (both Microsoft and non-Microsoft) o Server Applications – (i.e.: Microsoft IIS or SQL etc.) 4 o EUC Applications – (i.e.: Productivity Tools such as MS Office, Adobe Reader, and Web Browsers etc.) o Device Firmware

5. Software updates and patching

a. All IT systems (as defined in section 4), either owned by the Tradewalk of Tradewalk or those in the process of being developed and supported by third parties, must be licensed appropriately , supported by the manufacturer and be running up-to-date and patched Operating systems and application software.

b. Any IT system that is no longer licensed or supported by the manufacturer will be removed from the Tradewalk of Tradewalk network.

c. To protect the Tradewalk’s IT systems from known vulnerabilities, security patches must be deployed in a suitable time frame. Unless prevented by Tradewalk IT Procedures, patches should be deployed as per the following schedule: Vendor vulnerability classification Full deployment within (calendar days) Critical 14 High 14 Medium 21 Low 28

d. Where the deployment of ‘Critical’ or ‘High risk’ security patches within 14 days is not possible, either appropriate compensating controls or a temporary means of mitigation must be applied to reduce the exposure faced by the Tradewalk’s IT systems.

e. Third party suppliers must be prepared to provide evidence of up-to-date patching before IT systems are accepted into operational service.

f. New systems must be patched to the current agreed baseline before coming online in order to limit the introduction of new threats.

g. Servers must comply with the recommended minimum requirements that are specified by the Tradewalk of Tradewalk’s IT department which includes the default operating system level; service packs; hotfixes and patching levels. All exceptions shall be documented by the Tradewalk of Tradewalk’s IT department.

h. Microsoft patches are scheduled to deploy the first Monday after “Patch Tuesday”. This is the unofficial name used to refer to the day Microsoft releases its security patches which typically occurs on the second Tuesday of each month.

i. Servers managed by the Tradewalk of Tradewalk’s IT department will apply regular patches according to the IT department’s defined schedule:

j. Patches for key business systems, such Finance and the Student records systems are patched manually in a controlled manner.

k. All patches must be tested prior to full implementation since patches may result in unforeseen issues.

l. Testing will be carried out using a Test system that closely matches the production systems. Where there is no Test system then patch results from another non-key production system will be used and the results of any patch will be closely monitored for adverse effects.

m. User Acceptance Testing (UAT) of the business system must be completed after controlled patching completes.

n. A remediation plan that allows for the return to a working state must be in place prior to any patching. This could be either rolling back to a last known good state or fixing forward (e.g.: removing patches from the system and/or restoration of previous backup from Microsoft DPM or Azure Backup Service or deploying a more recent hotfix to correct a problem introduced by a patch).

o. Systems that are removed from the network as a result of insufficient patching will only be reconnected when it can be demonstrated that they have been brought up to date and are no longer present a risk to the Tradewalk of Tradewalk's network.

p. Those with patching roles as detailed in section 3 are required to compile and maintain reporting metrics that summaries the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk.

q. Tradewalk IT will endeavor to achieve 100% compliance for patching Operating Systems under its management.

r. Exceptions to the patch management policy require formal documented approval from the Deputy Director of IT.

s. This policy is subject to review every 6 months to ensure that it is accurate, effective and up to date.

Software/Hardware Policy

1. Acceptable use

This section defines the boundaries for the “acceptable use” of the Tradewalk’s electronic resources, including software, hardware devices, and network systems. Hardware devices, software programs, and network systems purchased and provided by the Tradewalk are to be used only for creating, researching, and processing Tradewalk-related materials. By using the Tradewalk’s hardware, software, and network systems Tradewalk policies,

2. Software

All software acquired for or on behalf of the Tradewalk or developed by Tradewalk employees or contract personnel on behalf of the Tradewalk is and shall be deemed Tradewalk property. All such software must be used in compliance with applicable licenses, notices and Contract

3. Purchasing

All purchasing of Tradewalk software shall be centralized with the information technology department to ensure that all applications conform to corporate software standards and are purchased at the best possible price

4. Software Standard

The following list shows the standard suite of software installed on Tradewalk computers (excluding test computers) that is fully supported by the information technology department

a. Microsoft Windows 10 and 11
b. Microsoft Office Outlook
c. Microsoft Office 2016
d. Microsoft Internet Explorer Edge
e. WinRAR
f. Greek
g. Resolute and Other Trading Application