Visualware®
Network Measurement and Quality Assessment

INFORMATION SECURITY POLICY

This Information Security Policy defines what is expected of employees, including all personnel affiliated with third parties authorized to work for/with the Company when receiving, transmitting or using information regardless of the information source and ownership.

All information and forms of information, including but not limited to, paper, digital, audio, and image/video, are valuable assets. This Information Security Policy serves to protect any and all information assets of the Company.

In addition, in this Information Security Policy, the main purpose required by the Company, is to establish and maintain adequate and effective information security practices for users, to ensure that the confidentiality, integrity and operational availability of information is not compromised.

Sensitive information must therefore be protected from unauthorized disclosure, modification, access, use, destruction or delay in service.

Each user has a duty and responsibility to comply with the information protection policies and procedures described in this document.

1. PURPOSE

The purpose of this policy is to maintain all information entrusted to or belonging to the Company in a secure environment.

This policy informs Company employees and other persons authorized to use Company facilities of the principles governing information retention, information use and information disposal.

2. SCOPE

This policy applies to all authorized persons of the Company who use computer systems or work with documents or information that concerns customers, suppliers or any other party for whom the Company has collected information in the normal course of business.

3. GOALS AND OBJECTIVES FOLLOWED

The goals and objectives of this policy are:

- Protect information from unauthorized access or use
- Ensure the confidentiality of information is maintained
- Maintain the integrity of information
- Maintain the availability of information systems for service delivery
- Comply with regulatory, contractual and legal requirements
- Maintain physical, environmental and communications security

- Dispose of information in accordance with company policy

4. AUTHORIZED USERS OF INFORMATION SYSTEMS

All users of the Company information systems must be formally authorized by the company systems administration department. Authorized users will be provided with a unique username and a password which must never be documented or disclosed to any other person.

Authorized users should take all necessary precautions to protect the Company information in their possession. Confidential, including but limited to, personal or private information must not be copied or transported without consideration of:

- the permission of the information owner
- the risks associated with loss or misuse of the information
- Transport requirements

5. ACCEPTABLE USE OF INFORMATION SYSTEMS

User accounts that provide access to the Company computer/application services must conform to the policies and practices documented in the Company Acceptable Use Policy (AUP). The Company computer services must never be used for personal activities unless authorized.

Unauthorized use of any system service may constitute a violation of the law, theft, and may mandate punishment by law. Therefore, unauthorized use of the Company computer system and services may constitute grounds for civil or criminal prosecution.

6. ACCESS CONTROL

The fundamental element of this Information Security policy is the control of access to critical information resources that require protection against unauthorized disclosure or modification.

Access control refers to the permissions assigned to persons or systems that are authorized to access specific resources. Access controls exist at different layers of the system, including the network. Access control is implemented by username and password. At the application and information level, other access control methods may be implemented to further restrict access.

Finally, application and information systems may restrict the number of applications and information services available to users based on work assignments.

7. NORMAL USER IDENTIFICATION

All users must have a unique username and password to access the systems, hereinafter referred to as credentials. A user password must remain confidential and under no circumstances should the password be shared with any other person regardless of position. Also, all users must comply with the following rules regarding password creation and maintenance:

- Passwords must be based on words that comprise a phrase or saying.

- Passwords must consist of 16 or more characters ensuring that one or more characters are lowercase, uppercase, numeric and non-alphanumeric (special characters such as $ or @).
- Passwords must never be written down or documented in any form.
- Accounts will be locked if a password is not changed within 30 days;
- Accounts will be automatically locked after 5 failed logon attempts;
- User accounts will automatically locked after 7 days without use.

Additional important points of note:

- Users are not allowed to access password files on any network infrastructure component. Password files on computer servers will be monitored for access. Copying, reading, deleting, or modifying a password file on any computer system is prohibited.
- Users will not be allowed credentials to logon as a System Administrator. Users who require administrator level of access to production systems must request a Special Access account.
- User names and passwords will be deactivated when the user is terminated, suspended, placed on leave, away on leave for more than 7 days or assigned a new position.
- Users will be responsible for all transactions occurring during any online session initiated by use of their credentials. Users must not allow another individual to use their computer system or otherwise share an online session without supervision.

8. CONFIDENTIALITY OF INFORMATION

Any information or documents that are not to be made public are automatically designated as "Company confidential for internal use only". All users who, in the course of their duties, handle this type of information must note::

- All confidential documents should be stored in locked file cabinets or rooms accessible only to those who have been granted access privileges.
- All electronic information that contains data that is clearly classed as personal, including but not limited to, name, address, telephone number, should be protected via a firewall, and passwords.
- User should clear their desks of confidential information before leaving their place of work.
- User should clear their computer monitors when they leave their workstations.
- All written information that is clearly classed as personal, including but not limited to, name, address, telephone number, should marked as "confidential."
- All information marked as confidential that is no longer required must be appropriately destroyed, e.g., shredded,
- User must not read, discuss or expose confidential information in public places.

- User should not transmit confidential information unless encrypted.
- User should not solicit confidential or personal client information, including but not limited to, social security numbers, bank account data, driving record, passport details, unless such information is integral to the purpose of the business application.
- All digital devices including but not limited to, computers, flash drives, hard drives, solid state drives, optical media, digital media, image/video media that are no longer required must be appropriately and securely destroyed.

9. RECOVERY OF INFORMATION

Any information asset that is maintained on one or more computer systems that is required to support any business process must be regularly backed-up such that the computer systems and the business processes, the computer systems support, can be reinstated when necessary.

As it relates to customer contracted information, the recovery processes must be tested for conformance to the disaster recovery requirements documented in the Customer Service Contract (CSC) on a regular basis. Recovery testing must validate both the Recovery Time Objective (RTO), the maximum of time allowed to reinstate service post a recover event, and the Recovery Point Objective (RPO), the maximum amount of data allowed to be lost post a recovery event (RPO).

Any recovery test that exceeds the RTO/RPO requirements documented in the CSC by more than 10% must be escalated to the customer account manager for action.

10. USER RESPONSIBILITIES

Any data security system relies on the users of the system to follow the procedures necessary for upholding data security policies. Users are required to report any weaknesses in the company computer security, any incidents of misuse or violation of this policy to their immediate line manager.

A user is therefore expected to:

- Comply with data security procedures and policies at all times;
- Protect their user IDs and passwords;
- Notify the Systems Administration department of any data security questions, issues, or concerns
- Assist the Systems administration department in mitigating identified data security issues;
- Ensure that all Information Systems that underwrite material business processes are backed up in a manner that mitigates both the risk of loss (RPO) and the costs of recovery (RTO)
- Be aware of the vulnerabilities of remote network access and their obligation to report intrusions, misuse or abuse to the Systems Administration department
- Be aware of their obligations if they store, secure, transmit and dispose of information concerning the activities or operations of the company, customers, suppliers or company products and services;

11. MONITORING OF COMPUTER SYSTEMS AND SERVICES

The company maintains the right and the capability to monitor electronic information created and/or communicated by persons using company computer systems and networks, including but not limited to e-mail, messaging and the usage Internet services.

Users of the systems should be aware that the company may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g., site access, time online, time of day etc.), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other digital communications are being used in compliance with the Company published Acceptable Use Policy (AUP).

12. SYSTEM ADMINISTRATOR

System administrators, network administrators and data security administrators will have access to the host systems, routers, hubs and firewalls necessary to perform their tasks.

All system administrator passwords must be deleted immediately after an employee who has access to these passwords has been terminated, dismissed or otherwise left the company's employment.

13. EMPLOYEE AGREEMENT ON DATA SECURITY POLICY

I acknowledge that I have received a copy of the COMPANY Information Security Policy. I have read and understand the policy. I understand that, if I violate the policy, I may be subject to disciplinary action, including termination. I further understand that I will contact my immediate manager if I have any questions about any aspect of the policy.

Dated: _____

EMPLOYEE/USER	COMPANY
_____	_____
Authorized Signature	Authorized Signature
_____	_____
Print Name and Title	Print Name and Title