IP Network Security Policy

Revision History	
Last updated	December 2020

Table of Contents

1. Policy Statement

Group Media provides a wide range of services to the MNO across African regions thereby require a secure IT infrastructure. Many of the computer systems supporting these services use the Wide Area Network (WAN) to transmit sensitive information such as critical transactions, personnel and subscriber records, and proprietary corporate data. The Group Media is committed to protecting the integrity, confidentiality, and availability of its information systems, the sensitive information these systems handle, and the privacy of subscribers' information, while providing for efficient and effective management of this information.

2. Definitions

Wide Area Network (WAN

For this policy, the WAN is defined to include all lines and devices used to terminate data communication services from a service provider. The WAN may also be referred to as the Provincial Data Network in various service provider agreements and other contracts signed with vendors. WAN devices may include hubs, routers, switches, wireless devices, or other devices. The Security Committee determines whether devices are classified as WAN or not. In this definition, personal computers, file servers, printers, or other Local Area Network (LAN) devices are not generally classified as part of the WAN. (See illustration on following page).

3. Corporate Network

For this policy, the Corporate Network includes the WAN, as defined above, as well as LANs including file servers, personal computers, printers, and other computing or data communications devices that are used by any department, office, agency, board, or commission within the Group Media. Any other connected organization is considered an External Entity requiring specific authorization to connect and access the Corporate Network and is required to abide by the WAN Security Policy and Standards, including any revisions, while connected. This definition of the Corporate Network is intentionally broad in scope to provide clear Committee boundaries for those charged with its security. (See illustration on following page).

Additional terms used in the body of this policy are defined in the glossary

The figure bellow is an Illustration of WAN and Corporate Network

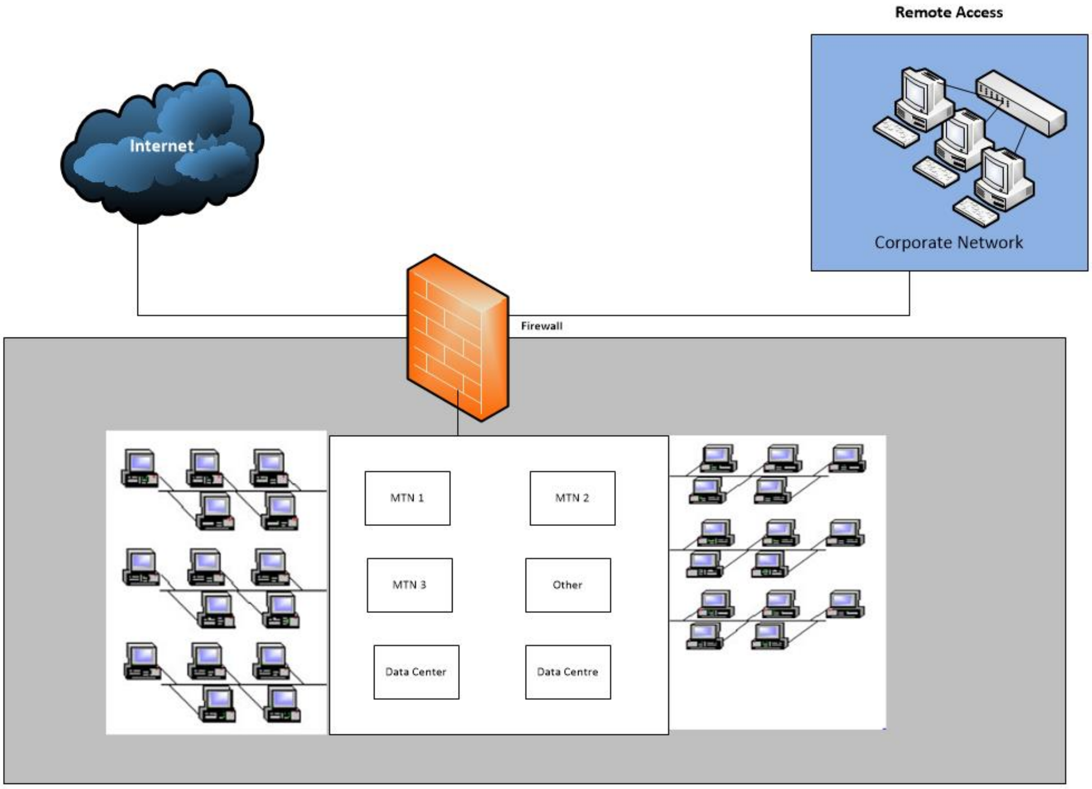

Figure 1: Conceptual Illustration of WAN Network, it is not intended as the true depiction of actual network

4. Policy Objectives

The objectives of this policy are to:

- Contribute to a secure WAN environment for all connected departments, offices, agencies, boards, and commissions.
- Provide a uniform security framework to secure the integrity, confidentiality, and availability of information and information systems, at the WAN level.
- Provide, in balance with operational requirements, legislative requirements, and information sharing agreements, the minimum WAN security requirements.
- Raise awareness of information and information technology security needs for all users of the WAN by providing the security principles, requirements, and rules of use.
- Define the clear roles and responsibilities of all users of the WAN, particularly WAN security staff.
- Provide a foundation to develop and implement additional policies and standards as may be required to address specific security issues.

5. Application

This policy applies to all Corporate Network connected MNO, offices, agencies and Client Organizations, and other authenticated users in an authorized area of the WAN such as commercial organizations (External Entities). Any content covered by departmental policies also covered by or in conflict with any content in this policy is superseded by this policy. Additionally, this policy supersedes any prior policies related to WAN security such as the Firewall Gateway Policy.

6. Policy Directives

Policy directives are the minimum mandatory requirements that shall be met by MNO and External Entities.

Overall Network Security Guidelines

a) Access and use of Group Media Contact network must be always consistent with Group Media Contact network security policies and standards.
b) Network security control measures are to be consistently applied to all employees, computer systems and communications systems
c) Information must be protected based on confidentiality, value, and criticality; regardless of the media on which it is stored or the methods by which it is moved.
d) Group Media Contact network security policies and standards will be reviewed on an annual basis, at a minimum, to ensure that they remain current. Security and Compliance Officer will review network security procedures and appropriate vendor guidelines on a semi-annual basis, at a minimum to ensure that the most current security measures are applied.
e) All Group Media Contact network components should be at least annually audited to make sure they remain in compliance with the Group Media Contact network security policies.
f) All employees must be provided with sufficient training and supporting reference materials to allow them to properly protect Group Media Contact network.
g) Security and Compliance Officer is responsible for identifying variances against generally accepted network security policies, and for promptly initiating corrective action.
h) All current Group Media Contact employees as well as well the new ones should be trained at least annually regarding the network security policies. Group Media Contact management must ensure that all employees read, understand, and sign the Group Media Contact network security policies.
i) Accountability and responsibility for following Group Media Contact network security policies on a day-to-day basis is every employee's duty.
j) Exceptions to network security policies and standards will only be made when the costs of implementing a standard exceed the security benefits or when the implementation will prohibit necessary Group Media Contact business activities.
k) Requests for changes to these statements contained in Network Security policies should be presented to and approved by the Group Media Contact management and Group Media Contact security consultant.

l) customer information (i.e., invoices) shall be treated with the highest level of sensitivity and any activities involving customer information shall be made in accordance with Group Media Contact security policies in the same way as confidential internal information.

Identification/Authentication

a) All accounts, user IDs and devices in the Corporate Network shall be uniquely identifiable.
b) IT systems within the Corporate Network shall authenticate all users, applications and devices except for those designed specifically for anonymous access. These exceptions require the approval of the Security Committee.

Access Controls/Authorization

LAN

a) Enable Port Security to protect the switch from MAC address table exhaustion.
b) Enable DHCP Snooping to secure DHCP services from being spoofed.
c) Enable Dynamic ARP Inspection to limit address resolution protocol (ARP) use to valid traffic.
d) Enable IP Source Guard to prevent IP host address spoofing.
e) Enable the spanning-tree Bridge Protocol Data Unit (BPDU) Guard to protect network availability.
f) Enable IPv6 Router Advertisement Guard to protect devices from communication with an IPv6 router connected to user access ports.
g) Enable IPv6 DHCP Guard to protect devices from communication with an IPv6 DHCP server connected to user access ports.

WAN

a) All access points to the WAN shall be approved by the Security Committee.
b) All physical and logical connections to the WAN intended to provide access by individuals or groups shall be approved by the Security Committee.
c) All WAN related address changes and configurations shall be approved by the Security Committee.
d) Any individual, office, or network connected to the Corporate Network shall require all employees to agree, through a signed or electronic agreement, to abide by the requirements outlined in the WAN Security Policy and Standards.
e) Requests for access to the WAN for an external entity shall be done through the Enterprise representative. The representative shall assume all responsibility for the entity requesting access.
f) Personnel who have access to sensitive information or are responsible for critical IT security functions such as network administrators and technical support staff require security screening.

7. Remote Access

a) Any remote access over untrusted networks shall use technology approved by the Security Committee to secure, monitor, and filter traffic.
b) All remote access to the WAN shall be authenticated, logged, and restricted to minimize the risk to WAN assets.
c) Infrastructure Service Management (ISM) of the Chief Information Office must ensure that remote access involving the WAN is monitored to protect the WAN security profile and confidentiality of sensitive information from unauthorized access and disclosure.
d) Any device which permits user-controlled access to the Corporate Network, such as a wireless modem, is not allowed except where permission is granted by the Security Committee.
e) All access to the Corporate Network shall occur through approved paths.
f) All users who use WAN resources remotely shall agree, through signed or electronic agreement, to abide by these requirements.

8. Firewalls

a) All communications between the Corporate Network and networks with different security profiles shall be protected by a network firewall approved by the Security Committee.
b) All firewalls and their configurations shall be provided and managed by the Security Committee except where the Security Committee approves Client Organizations to install and manage own firewall hosts.

9. Telecommunications Service Providers

a) All service providers contracting with Group Media such as suppliers of data communications or security services shall commit contractually to ensure that the WAN security profile is maintained.
b) All service providers contracting with Group Media Contact enterprises shall have access to the WAN Security Policy and Standards and agree to abide by them and ensure they are enforced within their organization.
c) Any exception to these directives shall be approved by the Security Committee and included as an addendum to the contract.

10. Contractors

a) All contracts or service agreements involving Corporate Network facilities, configuration, the management or any other application or server residing on the network shall include appropriate security clauses ensuring compliance with the WAN Security Policy and Standards.
b) All persons and organizations contracting with Group Media Contact (i.e., consultants, third-party sub-contractors, and casual and student employees) shall have access to the WAN Security Policy and Standards and agree to abide by them.

11. Physical and Environmental Security

a) An adequate environment (e.g., temperature, humidity, backup power supply) shall be provided to ensure optimum operation of the WAN and common infrastructure equipment as specified in the WAN documentation.
b) Physical controls shall be implemented to prevent unauthorized access to Corporate Network equipment including routers, switches, wiring racks, and network access servers.
c) The Security Committee shall have input into and final approval of all site design where WAN connectivity is being provided.
d) Access and use of Group Media Contact network must be always consistent with Group Media Contact network security policies and standards.
e) Network security control measures are to be consistently applied to all employees, computer systems and communications systems
f) Information must be protected based on confidentiality, value, and criticality; regardless of the media on which it is stored or the methods by which it is moved.
g) Group Media Contact network security policies and standards will be reviewed on an annual basis, at a minimum, to ensure that they remain current. Security and Compliance Officer will review network security procedures and appropriate vendor guidelines on a semi-annual basis, at a minimum to ensure that the most current security measures are applied.
h) All Group Media Contact network components should be at least annually audited to make sure they remain in compliance with the Group Media Contact network security policies.
i) All employees must be provided with sufficient training and supporting reference materials to allow them to properly protect Group Media Contact network.

j) Security and Compliance Officer is responsible for identifying variances against generally accepted network security policies, and for promptly initiating corrective action.

k) All current Group Media Contact employees as well as well the new ones should be trained at least annually regarding the network security policies. Group Media Contact management must ensure that all employees read, understand, and sign the Group Media Contact network security policies.

l) Accountability and responsibility for following Group Media Contact network security policies on a day-to-day basis is every employee's duty.

m) Exceptions to network security policies and standards will only be made when the costs of implementing a standard exceed the security benefits or when the implementation will prohibit necessary Group Media Contact business activities.

n) Requests for changes to these statements contained in Network Security policies should be presented to and approved by the Group Media Contact management and Group Media Contact security consultant.

o) customer information (i.e., invoices) shall be treated with the highest level of sensitivity and any activities involving customer information shall be made in accordance with Group Media Contact security policies in the same way as confidential internal information.

12. Time Synchronization

All devices on the Corporate Network shall synchronize with a common central time source.

13. Revocation/Termination of WAN Privileges

a) The Security Committee shall take appropriate action, including termination of any connection or activity, at any time where the Security Committee feels the security of the WAN is or could be severely comprised. When circumstances permit, the Security Committee shall consult with the application owner before taking action. The Security Committee shall make a full report of the actions taken and the reasons for such actions.

14. Change Control

a) All planned, scheduled changes to the WAN (power up, power down, configuration changes, and reset) shall be performed or authorized by the Security Committee.

b) A change control process shall be used to assess the security impact of major system upgrades and to support re-certification and accreditation. The change control process shall ensure that all system configurations and modifications are documented and retained in a secure environment for audit or future risk management considerations.

15. Security Risk Management Mechanisms and Planning

c) Security risk management based upon due diligence and due care shall be the primary basis to determine WAN security safeguards and residual risk and to maintain the accredited WAN security profile.

d) Re-assessments of the security profile shall take place if risk, system, or other relevant technological or organizational changes occur.

e) Before implementation, all new systems, as well as additions, deletions, or alterations to existing systems, shall be reviewed to ensure that the security profile of the Corporate Network is not compromised by the change.

f) The procurement and purchase of hardware and software must be reviewed by Network security management team. Development and users with elevated privileges must only use software that has been provided by a known and trusted person, supplier, or organization.

g) Group Media Contact communications networks will be designed so that no single point of failure, such as a central switching or core router, could disrupt network service essential to the continuity of business. Any single points of failure that exist on networks given less priority should be documented.

h) System designers and developers should always follow the network security policies for system designs

i) Security will be a fundamental design criterion used in all data network designs. While it is understood that other factors can and will influence the final design whenever possible security considerations must be given the utmost consideration in any design exercise.

j) Every system design must have provisions for error recovery and an audit trail. All computer-assisted processes must involve human intervention prior to initiating any action that could result in service interruption or sustained service downtime.

k) Only one primary function shall be implemented per system component and in case of virtualization environment one function shall be implemented per virtual machine.

l) All new system security controls must be tested prior to implementation.

m) Software in development must be kept strictly separate from production software. This separation must be achieved via physically and logically separate computer systems and networks where possible.

n) Test functions should be performed separately from production and development environments. The results of testing will be fully documented and securely maintained for a reasonable period.
o) All changes to production systems must follow the change control policies.
p) There shall be no restriction on use of open-source software and tools, provided appropriate legal review of the source code licenses has been granted, use is consistent with that license, and the software is appropriately tested.
q) Group Media Contact employees must not possess or use code-breaking software or hardware that allows illegal copying of proprietary software, discovery of passwords, or cryptanalysis of encrypted data.
r) The creation of any new network must be audited by Security and Compliance Officer and approved by the higher-level management.
s) The network architecture must be clearly documented.
t) Any changes to the existing architecture must follow the change control policies and procedures, and the relevant documentation must be updated immediately.
u) Network systems documentation (network diagrams, routing tables, IP addresses) are very sensitive information that will be restricted to authorized employees only.

v) All systems that store or process Group Media Contact or customers sensitive data will be protected using a firewall, or other approved network security devices, from public external networks.
w) Only authorized personnel will be allowed access to network equipment.
x) Different levels of access will be administered based on the job function, responsibility, and necessity of the employee's access.

16. Certification and Accreditation

a) IT system security certification and accreditation shall be performed on the Corporate Network (including all hardware and software that comprises the Corporate Network) throughout the planning, implementation, and operations life cycle.

17. Security Logs and Records

a) Appropriate logs shall be kept and reviewed as prescribed by the Security LAN Access Layer
b) Enable Port Security to protect the switch from MAC address table exhaustion.
c) Enable DHCP Snooping to secure DHCP services from being spoofed.
d) Enable Dynamic ARP Inspection to limit address resolution protocol (ARP) use to valid traffic.
e) Enable IP Source Guard to prevent IP host address spoofing.
f) Enable the spanning-tree Bridge Protocol Data Unit (BPDU) Guard to protect network availability.
g) Enable IPv6 Router Advertisement Guard to protect devices from communication with an IPv6 router connected to user access ports.
h) Enable IPv6 DHCP Guard to protect devices from communication with an IPv6 DHCP server connected to user access ports.
i) All actual or suspected security incidents shall be recorded and reported to the Security Committee.

18. Incident Reporting and Investigation

a) All Corporate Network security incidents shall be reported and investigated immediately by the infrastructure or application owner, Client Security Officer or designate, the Security Committee, or others as appropriate. The Security Committee shall notify other Client Security Officers who may be affected.
b) The Security Committee may also conduct a self-instituted secondary investigation as requested by the infrastructure or application owner, Client Security Officer or designate to determine if there are additional security issues and the appropriate solutions.

19. Security Information/Documentation

a) WAN infrastructure shall be documented as required by the Security Committee from time to time. The Security Committee shall be given access to this documentation on request to support WAN design security issues, disaster recovery operations, change control processes, diagnostic or hacker investigations, visual inspections, and security audits of the WAN infrastructure.
b) WAN security information and documentation including configuration, backups, and diagnostic information shall be password protected, physically stored under lock and key, and only released on the approval of the Security Committee. If located at a contractor site, the protective details and obligations shall be addressed in the contract.
c) Security information and documentation to be discarded, and which contains sensitive information such as passwords and IP addresses, shall be irretrievably

destroyed securely by shredding, permanent electronic deletion, or by other means approved by the Security Committee.

12. Monitoring/Surveillance and Privacy

a) The Security Committee shall monitor the WAN for performance and security purposes.
b) Monitoring initiatives designed for the WAN shall operate within the legislated requirements for the protection of personal privacy.
c) Access or monitoring of LAN segments shall be in co-operation with network administrators.
d) No person shall operate sniffers or other monitoring devices on the Corporate Network without the prior knowledge of the Security Committee.
e) Corporate Network monitoring shall not involve reading data content unless it is required in the performance of duties.
f) Where there is reason to believe that an individual is engaging in inappropriate activity on the Corporate Network the content of individual files may be read. This would only happen in an approved investigation by appropriate authorities.
g) Any investigation of data content shall be conducted following applicable human rights, and any applicable provincial and state legislation.

20. Security Training

a) The Security Committee shall provide training to all staff, Client Security Officers or designates, and others as necessary on WAN Security Policy and Standards including interpretation and application.
b) Client Organizations are responsible for the WAN Security training within their organization, and for any External Entities sponsored by them, required to ensure the performance of the security responsibilities outlined in the WAN Security Policy and Standards.

21. Accountabilities

General Managers (GM)

GM of each Client Organization is accountable for the overall security of all information within their jurisdiction.

Chief Information Officer

Chief Information Officer is additionally accountable for the strategic development and analysis of policy, standards, and processes for information security.

Security Policy Co-Ordinator

The Security Policy Coordinator is responsible for developing, monitoring, and proposing revisions to the WAN Security Policy and Standards in co-operation with WAN stakeholders.

Security Committee

The Security Committee is responsible for operational WAN security management and directs the implementation of the WAN Security Policy and Standards in co-operation with ISM, Client Security Officers or designates. The Security Committee evaluates and responds to all requests related to WAN access, services and security.

Client Security

A Client Security Officer or designate is the individual(s) assigned within each Client Organization to carry out security requirements and communications for their Client Organization and to work in co-operation with the Security Committee to ensure compliance with the WAN Security Policy and Standards.

Client Organization

A Client Organization is any department, office, agency, or enterprise in the Group Media connected to the Corporate Network and is required to abide by the WAN Security Policy and Standards.

External Entity

An External Entity is an organization having business with Group Media, sponsored by a Client Organization and authorized by the Security Committee, connected to the WAN. The External Entity shall agree to abide by the WAN Security Policy and Standards.

Managers And Delegated Staff

Managers and delegated staff, in addition to specific responsibilities cited above, shall have other specific responsibilities for such WAN aspects as availability, network upgrade and maintenance, security monitoring and incident reporting.

Organizations Hosting Wan Facilities

Organizations hosting WAN facilities such as routers, firewalls, wiring closets and other related components shall ensure that physical protection of WAN assets meets the WAN Security Policy and Standards.

22. Monitoring (of the WAN Security Policy)

General Manager

General Manager of each Client Organization is responsible for overall compliance with the WAN Security Policy and Standards.

Security Policy Co-Ordinator

The Security Policy Co-ordinator shall monitor WAN Security Policy implementation. This responsibility includes evaluating the suitability and effectiveness of the policy and standards. The Security Policy Co-ordinator shall co-ordinate any necessary remedial action to address issues reported by the Security Committee in the annual WAN security report. The Security Policy Co-ordinator shall also ensure that the policy and standards are formally reviewed at least every two years.

Security Committee

The Security Committee is responsible for monitoring the operational security of the WAN ensuring that the established security profile is maintained, and that changing environments, potential threats, and evolving technology are addressed. The Security Committee shall report annually to the Security Policy Co-ordinator on the WAN security environment, identified issues and security incidents, and the effectiveness of the WAN Security Policy.

Infrastructure Service Management (ISM)

ISM shall monitor compliance with the WAN Security Policy and Standards for all IT systems within their jurisdiction. ISM shall notify the Security Committee and the Security Policy Coordinator to request a policy review.

Client Security Officer or Designate

The Client Security Officer or designate shall monitor compliance with the WAN Security Policy and standards for all IT systems within their jurisdiction. The Client Security Officer or designate shall notify the Security Committee and the Security Policy Coordinator to request a policy review.

23. Enquiries

All enquiries, requests, or comments should be forwarded to

CIO:Chief Information Officer

24. Glossary

Access Control

A set of procedures performed by hardware, software and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access.

Accreditation

Approval by the responsible manager for the operation of an information technology system using a particular set of safeguards.

Authentication

The process of determining whether a person, workstation, system or procedure is eligible to access specific information, or to perform certain operations. Password validation, for example, is a form of authentication. Authentication may also be a measure meant to validate a transmission or message and the Committee of the originator.

Bastion Host

A server that is hardened against attack and can therefore be used as a critical component of network security. Firewalls and screening routers are examples of bastion hosts.

Certification

An examination by qualified personnel of an information technology system's implemented security safeguards against the system's security requirements.

Client Organization

See Accountabilities.

Confidentiality

The sensitivity of information or assets to unauthorized disclosure, recorded as highly confidential, confidential or protected, each of which implies a degree of injury should unauthorized disclosure occur.

Contractor

A third party involved in the direct management of the WAN or any part of it, quite often under a WAN management or data communications, service agreement. Contractors are required to abide by the WAN Security Policy and Standards.

Corporate Network

See Definitions

Due Care

Reasonable attention or caution which could be expected from an average person under the circumstances.

Due Diligence

A measure of prudence which could be expected from a reasonable and prudent individual having responsibility for some aspect of security risk management. It carries with it a higher level of responsibility than “due care”.

External Entity

See Accountabilities.

Firewall

A network security device positioned between networks with different security profiles that ensure all communications attempting to travel between the networks conform to the configured security profile

Integrity

The quality or condition of being accurate or complete.

Modem (Modular-Demodulator)

A device that converts digital signals used by computers and analogue signals used by the telephone or related telecommunication system which enables computers to communicate remotely. In the WAN Security Policy and Standards, a modem includes any telecommunications device such as a dial-up modem, cable modem, dedicated line modem, wireless device or digital subscriber line (DSL) device.

Monitor

The activity to ensure that information and assets, or the safeguards protecting them, are checked by security staff or electronic means with sufficient regularity to satisfy the WAN Policy and Standards.

Security Profile

A minimum acceptable level of security for the WAN established by the implementation of the WAN Security Policy and Standards.

Security Committee

See Accountabilities. *All references to the Security Committee in this document means the Security Committee or a delegate appointed by the CIO from time to time.*

Security Incident

An occurrence or situation that results in a compromise of sensitive information, assets, functionality, or a loss of availability or integrity.

Security Risk Management

The process by which resources are planned, organized, directed and controlled to ensure the risk of operating an IT system remains within acceptable bounds at optimal cost.

Service Provider

A third party involved in the direct management of the WAN or any part of it, quite often under a WAN management or data communications contract. Exceptions to the WAN Security Policy and Standards, if applicable, shall be documented in the service agreement.

Time Synchronization

Process of ensuring that all devices on the WAN have the same time to ensure the accuracy of records and logs.

Threat

Any potential event or act that could cause one or more of the following to occur : unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets, services, or injury to people. A threat may be deliberate or accidental.

Threat and Risk Assessment

An evaluation, based on the effectiveness of existing or proposed security safeguards, of the chance of vulnerabilities being exploited.

Untrusted Network

A network, such as the Internet, that has no basis for a user to have any confidence and assurance in its inherent security.