

MICROTEAM LIMITED DATA SECURITY POLICY – R1.0. May 2006

Introduction

The purpose of this document is to define the Microteam Limited Data Security Policy. Data is considered a primary asset and as such must be protected in a manner commensurate to its value. Data security is necessary in today's environment because data processing represents a concentration of valuable assets in the form of information, equipment, and personnel. Dependence on information systems creates a unique vulnerability for our organization.

Security and privacy must focus on controlling unauthorized access to data. Security compromises or privacy violations could jeopardize our ability to provide service; lose revenue through fraud or destruction of proprietary or confidential data; violate business contracts, trade secrets, and customer privacy; or reduce credibility and reputation with its customers, shareholders and partners. This policy therefore discusses:

- ← ■ Data content
- ← ■ Data classification
- ← ■ Data ownership
- ← ■ Data security

The main objective of this policy is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all of our and all customer data assets that exist, in any of our processing environments. The processing environment is considered to be, collectively, all applications, systems, and networks that we own or operate or that are operated by our agents.

This policy defines the Microteam Ltd overall security and risk control objectives that we endorse. The premise for the policy can be stated as:

“Other than data defined as public, which is accessible to all identified and authenticated users, all data and processing resources are only accessible on a need to know basis to specifically identified, authenticated, and authorized entities.”

This embodies the principle of least privilege.

This document forms part of your conditions of employment for employees, a part of the contractual agreement for vendors, suppliers, and third party processor or agents, hereafter referred to as vendors. All parties must read the policy completely, and confirm that they understand the contents of the policy and agree to abide by it.

Breach of Policy and Enforcement

A breach of this policy could have severe consequences to Microteam Ltd, its ability to provide services, or maintain the integrity, confidentiality, or availability of services.

Intentional misuse resulting in a breach of any part of this policy will result in disciplinary action at the discretion of Microteam Ltd senior management. Severe, deliberate or repeated breaches of the policy may be considered grounds for instant dismissal; or in the case of a Microteam Ltd vendor, termination of their contracted services. All employees and vendors are bound by these policies and are responsible for their strict enforcement.

Scope of the Policy

This policy applies to all Microteam Ltd and customer data assets that exist in any Microteam Ltd processing environment, on any media during any part of its life cycle. The following entities or users are covered by this policy:

- ←▪ Full or part-time employees of Microteam Ltd who have access to Microteam Ltd or customer data.
- ←▪ Microteam Ltd vendors or processors who have access to Microteam Ltd or customer data.
- ←▪ Other persons, entities, or organizations that have access to Microteam Ltd or customer data.

Data Life Cycle

The security of data can be understood through the use of a data life cycle. The typical life cycle of data is: generation, use, storage and disposal. The following sections provide guidance as to the application of this policy through the different life cycle phases of data.

Users of data assets are personally responsible for complying with this policy. All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access. Data must only be used in a manner consistent with this policy.

Data Usage

All users that access Microteam Ltd or customer data for use must do so only in conformance to this policy. Uniquely identified, authenticated and authorized users must only access data.

Each user must ensure that Microteam Ltd data assets under their direction or control are properly labeled and safeguarded according to their sensitivity, proprietary nature, and criticality.

Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights.

Data Transmission

All users that access Microteam Ltd or customer data to enable its transmission must do so only in conformance to this policy.

Data Storage

All users that are responsible for the secure storage of Microteam or customer data must do so only in conformance to this policy.

Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights.

Data Disposal

Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights during the disposal process. Microteam uses software that is certified by Her Majesty's Government and US Department of Defense for data erasure. Any device that is found to be inoperable or cannot be erased is destroyed by secure shredding.

The Data Security department must develop and implement procedures to ensure the proper disposal of various types of data. These procedures must be made available to all users with access to data that requires special disposal techniques.

Data Security Policy Statement

This section describes the particulars of the data security policy. This section should provide sufficient information to guide the development and implementation of guidelines and specific data security procedures.

Goals

This policy has been written with the following goals in mind:

- ←■ To educate Microteam Ltd users and vendors about their obligation for protection all data assets.
- ←■ To ensure the security, integrity, and availability of all Microteam Ltd and customer data.
- ←■ To establish the Microteam Ltd baseline data security stance and classification schema.

Processing Environment

The Microteam Ltd processing environment that this policy applies to is comprised of:

- ←■ **Applications** – Application software is system or network-level routines and programs designed by (and for) system users and customers. It supports specific business-oriented processes, jobs, or functions. It can be general in nature or specifically tailored to a single or limited number of functions.
- ←■ **Systems** – A system is an assembly of computer hardware (e.g., sub-networks, application servers, file servers, workstations, data, etc.) and application software configured for the purpose of processing, handling, storing, transmitting, and receiving data, that is used in a production or support environment to sustain specific applications and business organizations in their performance of tasks and business processes.
- ←■ **Networks** – A network is defined as two or more systems connected by a communication medium. It includes all elements (e.g., routers, switches, bridges, hubs, servers, firewalls, controllers, and other devices) that are used to transport information between systems.

Data Security Responsibilities

The Data Security organization is responsible for:

- ←■ Defining the security requirements, controls and mechanisms applicable to all data assets.
- ←■ Defining the methods and guidelines used to identify and classify all data assets.
- ←■ Defining the procedures for identifying data owners for all data assets.
- ←■ Defining the labeling requirements for all data assets.
- ←■ Defining all other data security usage, processing, transmission, storage and disposal processes and procedures.
- ←■ Defining the procedures necessary to ensure compliance to this policy by all Microteam Ltd users and vendors.
- ←■ Facilitating the evaluation of new regulatory, legal, and also best practice requirements as they are mandated or become recognized in industry.

The *Data Security*, *Network Operations* and *Systems Administration* organizations must ensure the activation of all security mechanisms.

Management Responsibilities

Other organizations within Microteam Ltd also have various responsibilities for ensuring compliance with this policy, such as:

- ←■ All individual departments must ensure that staff complies with this policy.
- ←■ The *Network Operations and Systems Administration* organizations must ensure that adequate logs and audit trails are kept of all data access.
- ←■ The Data Security, *Network Operations and Systems Administration departments* must ensure the activation of all security mechanisms.
- ←■ The *Risk Management department* is responsible for communicating business requirement and issues for business processes and the data those include, to ensure their correct data classification.
- ←■ The internal audit department is responsible for regularly evaluating the data classification schema for consistent application and use.

Other Responsibilities

Other departments have responsibilities to comply with this policy, such as:

- ←■ All Microteam Ltd agents, vendors, content providers, and third party providers that process customer data must have a documented security policy that clearly identifies those data and other resources and the controls that are being imposed upon them.
- ←■ All Microteam Ltd agents, vendors, content providers, and third party providers that access the Microteam Ltd processing environment and its data or provide content to it must have a security policy that complies with and does not contradict the Microteam Ltd security policy.
- ←■ All agents, vendors, content providers, and third party providers must agree not to bypass any of our security requirements.

Documentation

This policy requires procedures be developed, managed and performed. As such, written documentation must be developed for all procedures necessary to fulfill this policy including:

- ←■ The management of all userids on all platforms.
- ←■ The management of all access control lists on all platforms.
- ←■ The execution and review of all audit trails.
- ←■ All incident response and reporting.
- ←■ All other tasks necessary to support this policy.

Policy Review

It is the responsibility of the Data Security department to facilitate the review of this policy on a regular basis. Because of the dynamic nature of the Internet, this policy should be reviewed annually. Senior management, Systems administration, and Legal should, at a minimum, be included in the annual review of this policy.

Data Content

The nature of specific data content that exists in the processing environment, and the controls that should apply to these, is dependent upon various factors. This policy does not mandate or endorse particular data content. Rather, the business decision process used to evaluate the inclusion or exclusion of particular data content should consider those items listed below. Regardless as to the specific data content that exists in the environment, all aspects of this policy must be enforced. Considerations for evaluating data content include:

- ←■ Legal and regulatory obligations in the locales in which we operate.
- ←■ Can privacy, confidentiality, security, and integrity of the data be ensured to the satisfaction of customers and legal authorities?
- ←■ Is it in line with our business goals and objectives?

- ←■ Do customers require or demand access to specific data content.
- ←■ What is common local practice? (e.g., pornography is legal in some communities but strongly frowned upon in others.)
- ←■ What rules govern the movement across international boundaries of different data content, and do we have in place controls to enforce these rules?

Data Classification

Data classification is necessary to enable the allocation of resources to the protection of data assets, as well as determining the potential loss or damage from the corruption, loss or disclosure of data.

To ensure the security and integrity of all data the default data classification for any data asset is either Confidential Customer Data or Proprietary Company Data.

The Data Security organization is responsible for evaluating the data classification schema and reconciling it with new data types as they enter usage. It may be necessary, as we enter new business endeavors, to develop additional data classifications.

All data found in the processing environment must fall into one of the following categories:

- ←■ **Public Company Data** – Public company data is defined as data that any entity either internal or external to Microteam Ltd can access. The disclosure, use or destruction of Public company data will have limited or no adverse affects on Microteam Ltd nor carry any significant liability. (Examples of Public company data include readily available news, stock quotes, or sporting information.)
- ←■ **Proprietary Company Data** – Proprietary company data is any information that derives its economic value from not being publicly disclosed. It includes information that Microteam Ltd is under legal or contractual obligation to protect. The value of proprietary company information to Microteam Ltd would be destroyed or diminished if such information were disclosed to others. Most Microteam Ltd sensitive information should fall into this category. Proprietary company information may be copied and distributed within Microteam Ltd only to authorized users. Proprietary company information disclosed to authorized external users must be done so under a non-disclosure agreement. (Examples of Proprietary company data include company policies, sales plans, and application source code.)
- ←■ **Confidential Company Data** – Confidential Company Data is information that is not to be publicly disclosed, regardless of its economic value. The disclosure, use, or destruction of Confidential Company Data can have adverse affects on Microteam Ltd and possibly carry significant civil, fiscal, or criminal liability. This designation is used much less frequently. It is used for highly sensitive information whose access is restricted to selected, authorized employees. The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know for the information. Company confidential information must not be copied without authorization from the identified owner. (Examples of Confidential Company Data include company strategic plans or cryptographic keys.)
- ←■ **Confidential Customer Data** – Confidential customer data is defined as data that only authorized internal Microteam Ltd entities or specific authorized external entities can access. The disclosure, use, or destruction of confidential customer data can have adverse affects on Microteam Ltd and their relationship with their customers, and possibly carry significant liability for both. Confidential customer data is entrusted to and may transit or is stored by Microteam Ltd (and others) over which they have custodial responsibility but do not have ownership. (Examples of Confidential customer data including customer bank or brokerage account information, cryptographic keys, or other data considered private.)
- ←■ **Public Customer Data** – Public customer data is defined as data that any entity either internal or external to Microteam Ltd can access. The disclosure, use, or destruction of Public customer data will have limited or no adverse affects on Microteam Ltd or the customer, and carry no significant liability. Public customer data is entrusted to, and may transit or be stored by Microteam Ltd (and others) over which they have custodial responsibility but do not have ownership. (Examples of Public customer data include emails, public key certificates or other customer data that is readily available through other public channels or records.)

Data Ownership

In order to classify data it is necessary that an owner be identified for all data assets. The owner of data is responsible for classifying their data according to the classification schema noted in this policy. If an owner cannot be determined for a Microteam Ltd data asset, the Data Security organization must act as its custodian. The default classification for all data not classified by its owner must be either confidential customer data or Proprietary company data.

The Data Security department is responsible for developing, implementing, and maintaining procedures for identifying all data assets and associated owners.

The owner of all customer data is the individual owner who generates or is assigned ownership of that data. (Data such as public key certificates generated by an external Certificate Authority but assigned to a specific customer are considered owned by that customer.

Non-disclosure Agreements

On occasion, data assets may need to be released to entities outside of Microteam Ltd. When a legitimate business reason exists for releasing sensitive information, a written Non-Disclosure Agreement (NDA), requiring the data recipient's agreement to maintain that data in confidence and restrict its use and dissemination, must be obtained before disclosing the data.

Data Security Principles

Microteam Ltd's business goals, objectives, and needs for security can be derived from three principles: accountability, authorization, and availability. These three principles emphasize the need for security to function properly in Microteam Ltd's processing environment, which is comprised of applications, network, and system resources. Non-compliance with these principles can have serious, adverse, and deleterious affects on Microteam Ltd.

In the context of this policy, the following provides the overall concepts or security principles for which all users and vendors are responsible. It is the responsibility of the Data Security department to define the specific mechanisms necessary to support these principles.

Accountability

All network, system, and application events should be attributable to a specific and unique individual. It should be possible to attribute a responsible individual to every event through an identification service and to verify that the individual so assigned has been properly identified through an authentication service. It must also be possible to trace any event so as to reconstruct the time, place, and circumstances surrounding it through an audit service.

In this context identification refers to a security service that recognizes a claim of identity by comparing a userid offered with stored security information. Authentication refers to a security service that verifies the claimed identity of the user, for example a password. Auditability refers to a security service that records information of potential security significance.

Authorization

All network, system, and application events must only result from allowable actions through access control mechanisms. Permission may be derived directly from an individual's identity, or from a job classification or administrative privilege based on that individual's identity. The principle of "least privilege" specifies that individuals only be granted permission for actions needed to perform their jobs.

Limiting actions to those properly authorized protects the confidentiality and integrity of data within the Microteam Ltd processing environment.

In this context access control refers to a security service that allows or denies a user request based on privilege, group information, or context. Confidentiality refers to a security service that prevents disclosure of information to unauthorized parties while the information is in use or transit, or being storage or destroyed.

Availability

All permitted activity should operate with reliability. The data necessary to carry out such events must be readily retrieved and correct with high confidence. All results of an event must be completed, unless the event is aborted in its entirety. The results of an event should not depend in unexpected ways on other concurrent events. The security services themselves must be documented and easily administered.

In this context integrity refers to a security service that guarantees data has not been altered, deleted, repeated, or rearranged during transmission, storage, processing, or recovery.