Corporate Data Security Policies

Corporate Data Security Policies

Content

Introduction

Corporate Data Security is to define the Micro team Limited Data Security Policy. Data is considered 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 Micro team Ltd overall security and risk control objectives that we endorse. The premise for the policy can be stated .

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.

Secure Drives are a unique solution to the problem of employee resistance to using encryption in that there is no software to install, little or no training is required, no changes to current IT systems or infrastructure are necessary and there are no changes to current, established working practices or workflow.

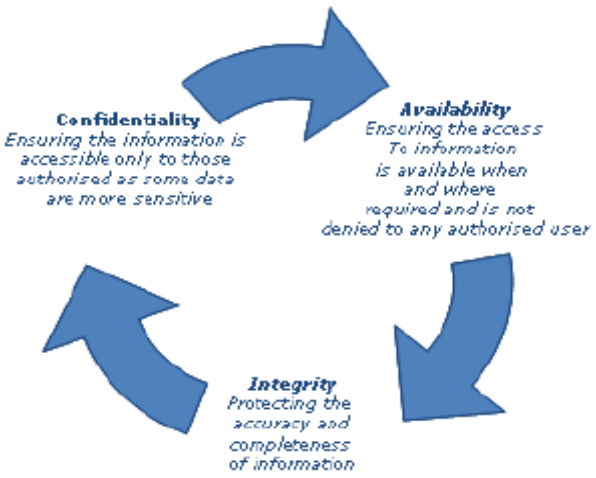
Secure Drives achieve this by balancing usability and security with productivity and compliance.

This document is organized into sections, which may or may not be applicable depending on where you are in your security policy development process. Feel free to skip ahead to the section that applies best to you.

Corporate Data Security Challenges

The following are some of the major enterprise concerns related to the use of Secure drives . Data leakage: to limit data leakage, organizations should regulate the use of Secure drives, eventually allowing the use of company-authorized Secure drives only .Regulatory and security standards compliance challenges: having enterprises take care of secure USB flash drives usage will help in complying with the three aspects of security (i.e. confidentiality, availability and integrity) and some security standards and/or compliance framework (e.g. Sarbanes-Oxley, PCI data security standards etc.)

Lost data and support costs: security policy could help enterprises recuperate stolen or lost data which occur even when security measures are in place, decreasing the costs of ownership and support.



The role of Information Security Officer was assigned to a diverse selection of individuals, ranging from directors, compliance officers, dedicated information security officers, and IT personnel.

Purpose and Scope

This Secure Drives white paper is designed to provide an up-to-date understanding of the data security threat landscape together with an overview of workflow problems and logistical issues surrounding current data encryption and automated backup technology. The paper will focus in particular on the problems associated with sensitive data which has to be stored securely by end users at the point of use and regularly backed up. This paper explains the Secure Drives solution and is aimed at personnel who are responsible for implementing, performing or reviewing information security processes, managing data loss policies, developing supply chain compliance strategies and supervising non-technical data users.

Foreword

Practice in data security should be regarded as a pre-requisite of effective and successful. This is principally because good data security is an integral part of private clients' confidence in working with SecurDrive.

Corporate Policies and Procedures Acknowledgement

I understand that I am expected to read and comply with the policies and procedures outlined in the Corporate Human Resources Policies and Procedures, available on my Block, as well as all Company policies and procedures applicable to my position. I understand that the Company may amend its policies and procedures at any time and that I must comply with all policies and procedures as amended. I also understand that if I have questions concerning any of the policies or procedures of the Company. I understand that violating the Company's policies, including, without limitation, those specifically identified below, can result in disciplinary action up to and including termination of my employment or, if I am a contingent worker, my assignment.

1. 1. My access to private, personal data (including sensitive data information) is limited to my need to know based on the function of my job responsibilities at the University.
2. I have completed the PCIDSS Training module and understand the responsibility I have to protect and safeguard private data information entrusted to me.
3. I have been informed of the Incident Response Plan and understand that if there is an occurrence when I suspect a breach in data security or personal data, I will report it immediately to the appropriate personnel.
4. I understand that any violation of the Data Security Standards listed and agreed to in this acknowledgement form can result in disciplinary action, including dismissal from employment, as well as criminal penalties or civil liability.

The Economics of Compliance

Secure Drives have been designed and engineered from the ground up from the individual end users point of view. It's mainly individuals who cause data loss, it's individual end user behavior which has to be sustainably modified and it's individuals who choose whether to comply or not with the security policies governing their immediate work context.

Individuals choose whether or not to comply with security guidelines based on risk and reward or cost and benefit. There is a natural limit to the amount of effort users will expend on compliance unless there is a corresponding benefit.

Modern digital encryption came out of the US military in the 1970s and 1980s. The inflexible command and control structure of its original development environment created the encryption structures and landscape we see today.

Within a fully integrated public or private organization, with a standardized IT structure, encryption offers nearly unbreakable information security. It's possible to demonstrate mathematically that it is computationally impossible to retrieve encrypted data without the encryption keys. However even within a tightly integrated IT environment everyday practical issues in the deployment, maintenance and use of encryption technology have limited the business benefits and impaired the efficiency of business operations. Misapplied encryption increases risk, decreases security, incurs unnecessary costs and reduces efficiency.

Until recently it has been almost impossible for non-technical end users, with dissimilar I.T. skills and differing attitudes to data protection to securely store, use and backup confidential or personal data.

This paper targets IT departments, in particular IT managers and professionals, to ensure the ability to secure information on the network as well as the opportunity to manage data which enter and leave the company via these mobile devices. It also targets corporate end-users in general, to raise awareness of the risks related to the use of Secure drives. This document does not cover the associated legal aspects. Moreover, it should not be seen either as a comprehensive source of all risks associated with the use of personal USB flash drives for work related purposes or a technical guideline to secure standards or solutions.

1. Most organizations had up to date security policies that covered the key areas of data Security Policies were an important but effective means of communicating security responsibilities to staff.

2. Although risk assessments were being performed, when organizations Considered data Security risk they tended to note it as a single generic item. This Narrow approach does not support effective assessment of such a complex Category and a more granular approach are needed.

3. For the majority of organizations, staff was not given adequate security awareness Training. Training was either minimal or only performed once at the time of joining.

After a preliminary analysis of the results we identified key areas of focus and selected a cross-section of licensees for onsite review. The onsite focus areas were:

? security governance

? third party risk

? data leakage prevention

? staff security awareness

Security Policies

A security policy is a strategy for how your company will implement Information Security principles and technologies. It is essentially a business plan that applies only to the Information Security aspects of a business.

A security policy is different from security processes and procedures, in that a policy will provide both high level and specific guidelines on how your company is to protect its data, but will not specify exactly how that is to be accomplished. This provides leeway to choose which security devices and methods are best for your company and budget. A security policy is technology and vendor independent – its intent is to set policy only, which you can then implement in any manner that accomplishes the specified goals.

A security policy should cover all your company's electronic systems and data. As a general rule, a security policy would not cover hard copies of company data but some overlap is inevitable, since hard copies invariably were soft copies at some point. Where the security policy applies to hard copies of information, this must be specifically stated in the applicable policy.

A security policy must specifically accomplish three objectives:

1. It must allow for the confidentiality and privacy of your company's information.
2. It must provide protection for the integrity of your company's information.
3. It must provide for the availability of your company's information.

Data Security policy Benefit in Corporate

- Ensure Employee Report Cases of lost of Stolen SecurDrive to the IT Department
- Conduct a Damage Assessment for Every SecurDrive that Goes Missing
- Establish how and where they went missing
- Review your policies guideline to ensure major sources of loss are covered
- Highlight potential risk associate with the innocent use of SecurDrive by employees and for other less legitimate purpose such as smuggling information out of the Company
- Take specials measures for business units/Departments which are handling sensitive data
- Monitor and report incidents on regular basis
- Train and send out reminders to employees
- Benchmark your performance against other similar enterprises

Benefits

An overview of any benefits linked to a secure use of SecurDrive will help and lead the enterprise to better decide about this matter.

The following benefits were identified.

Enhance and boost employee productivity through mobility and remote connectivity Flexible and secure solution will

- protect Corporate assets
- reduce total cost of ownership
- prove that device were encrypted when stolen or lost

Defend enterprises from data leakage

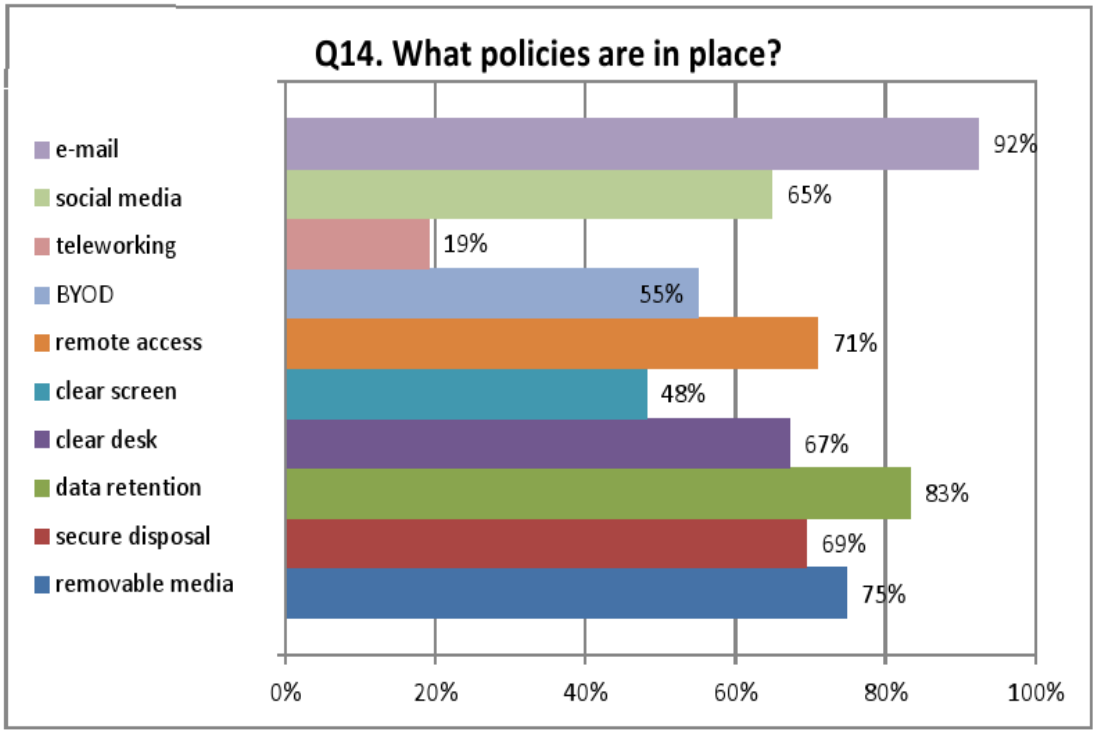
Enforce mandatory company-wide security policies

- track all activity on SecurDrives

Comply with the three pillars or classifications of information security - confidentiality, availability and integrity- and security standards.

Policies are in place

Respondents used a wide range of policies documents to convey data security obligations to their employees. It was also reassuring to see that 68% had reviewed security policy documents for policies to be effective in a rapidly changing area like data security; they need to keep up with the latest trends in technology, so regular reviews are essential.



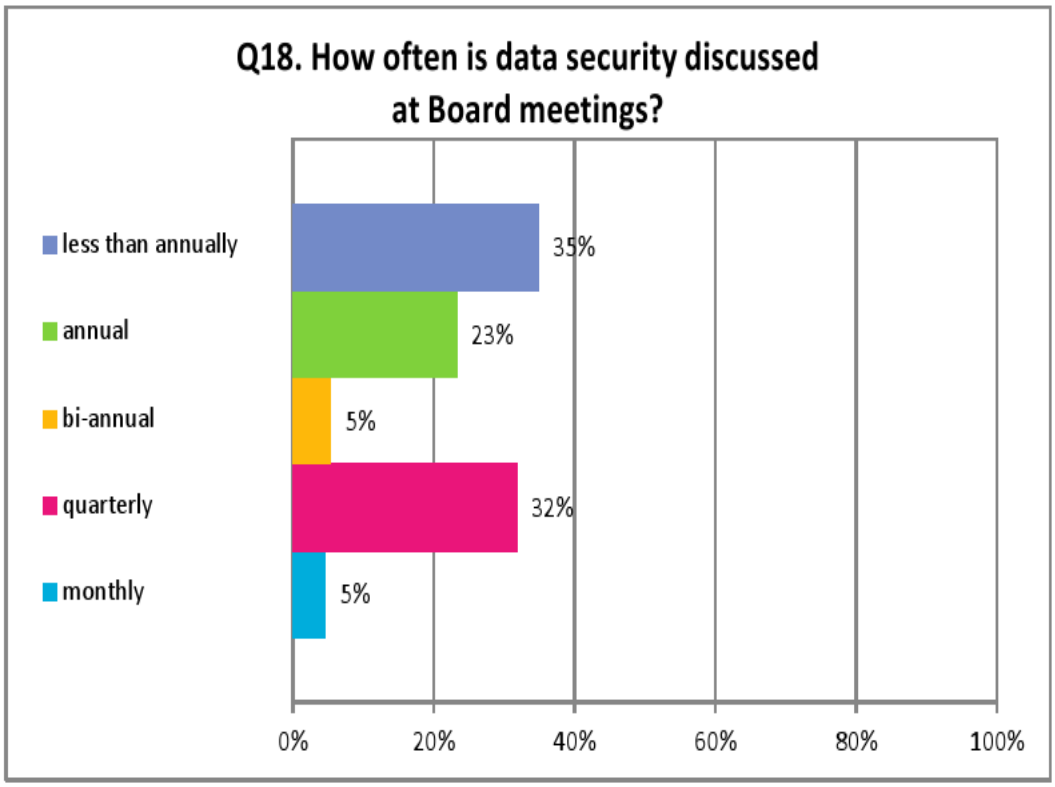
For the majority of organizations policy coverage appeared to be quite extensive. In particular it was encouraging to see that social media and BYOD (bring your own device) scored quite highly (65% and 55% respectively), despite the relative immaturity of these technologies.

Governance

Corporate Governance Issues

Every organization, and indeed individual, faces a constant barrage of data security threats. These threats and the controls needed to mitigate them are constantly evolving. It is therefore vital that the

Board keeps up to date on these matters and gives them due consideration and attention. Unless the Board is fortunate enough to have a sufficient understanding of data security, then it should seek advice from service providers and other specialists.



Recommendations and possible software and hardware solutions

There are a number of recommendations and software and hardware solutions to ensure the secure use of Secure drives.

Implement a risk assessment methodology to ensure the correct controls to minimize risks throughout the lifecycle of the devices . A risk assessment will allow for understanding in detail the risks related to the use of Secure drives and costs providing the basis to develop a strategy for closing these gaps .

Implement security policies/guidelines around the use of Secure drives and storing of corporate data on to a personal Secure drive.

Develop a company security policy which has every employee signing an agreement for not connecting their personal Secure drive to the network and transport data. Eventually allow the use of corporate.

- Make staff aware of the important role they play in security.
- Conduct a security audit.
- Use strong and multiple passwords.
- Encrypt your data.
- Back up. Have security policies.
- Implement a multiple-security-technology solution.

Secure drives, specifying employee responsibilities and rules for safe use and blocking devices that have no valid business use . Thus define what types of hardware are allowed to access the network.

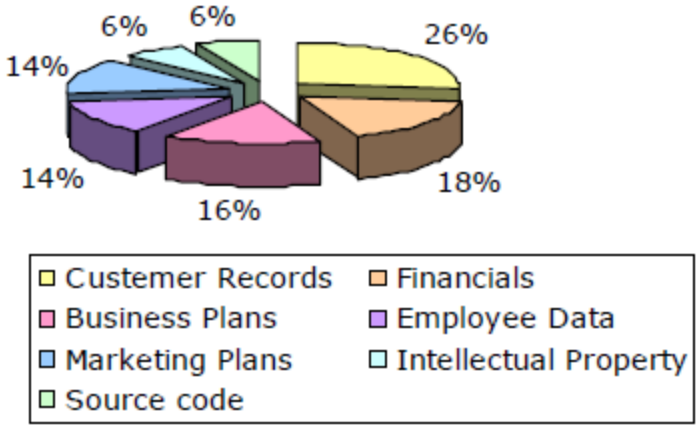
Corporate policies should be comprehensive but not so restrictive as to impede employee productivity.

Corporate Data on SecurDrives

USB drives are solutions to store and manage enterprise data within and outside the enterprise
environment. USB drives are also known as a keychain drive, flash drive or disk-on-key. They are
plug-and-play portable storage devices that use flash memory and are lightweight enough to attach
to a key chain.

USB drives are a powerful and popular tool for mobile professionals in enterprises or government
agencies as they have:

- small size and light weight
- fast speed — 24MB/s
- big capacity
- low price
- plug-and-play functionality.



Executive Summary

corporate end-users have increasingly needed to SecurDrive connected, taking work home or out of the office to keep up their productivity. Staff needs to be able to synchronize files between a computer and the drive to allow key data to be backed up and available for use on the road or on other PCs .

In particular, personal storage devices such as SecurDrive have gained in capacity and have become ubiquitous in the enterprise environment . However, these SecurDrives are usually lacking insecurity, control and management tools and, in most cases, their use is not covered by a corporate policy foreseeing audit, backup, encryption or asset management.

Recent events have raised concern, leading organizations to understand that to secure corporate information stored on personal Secure drives, new policies and technologies must be put in place. Often the measures organizations take to secure information stored on mobile devices are inadequate. Enterprises with highly regulated or sensitive data should consider controlling the use of plug-and-play devices. However, awareness of the risks and available safeguards is the first line of defense for security .

> This document gives a brief outline of the corporate data which is susceptible to security breaches incidents, and highlights potential risks associated with the innocent use of Secure drives by employees of enterprises and also other less legitimate purposes such as smuggling information out of the company. Furthermore, it lists good practice guidelines which aim at helping readers to overcome obstacles within their organizations. The first step is to set clear security policies and make employees aware of them.

Solution of Corporate

SecureDrive provides 2GB to 64TB secure mobile data solutions to meet security policies of various organizations.

As employees and business functions become increasingly mobile, the need to protect business and user data becomes more paramount.

SecureDrive provides a range of secure data drives with the highest level of protection against loss of data.

Customizing

SecureDrive provides Government and Corporate businesses customized portable secure data solutions to meet their needs:

1.**Encryption choice** - We can provide you with AES 128-bit or AES 256-bit encrypted devices to meet your company's encryption policies.

2.**Capacity choice** - We can provide you with 2GB to 64TB capacity devices to meet your company's secure data storage needs.

3.**Laser Etching** - We can laser etch your company name, logo or any other message on the anodized aluminum sleeve of the detacher/detacher Persona/detacher SSD.

4.**Product Branding** - We can completely re-brand our devices to reflect your company's individual look - minimum order quantities (MOQ) applies.

5.**Pre-programmed PINs**- We can supply our products with your own unique User/Admin PINs already pre-programmed into the device in compliance with your corporate password policies.

6.**Software** - We can pre-install documents, software and portable applications on any storage device ready for your use.

The Technology

Access to software and classified data should be restricted to authorized personnel only. Authentication with passwords and tokens are common techniques for access protection, and different authorization profiles are often applied to different users according to their roles. Audit trails are supplementary to authentication, and comprehensive activity logs provide useful information for refining the effectiveness of security measures. Data Encryption provides another level of protection to guard against unauthorized data access.

Technical guidelines and technical implementation are typically technology specific

1. [Complete as appropriate] is the standard product.
2. Strong, industry best practice defined cryptographic standards must be employed. AES-256 is an approved implementation.
    a. Scope of possible policies
    b. Assessing the Risks

Developing Security Policies for protecting Corporate Assets

o Computer user policy and user training

o Network Policy

o Remote access policy

o Physical Security Policy

1. Synchronization with Windows credentials will be configured so that the pre boot environment is matched to the user's credentials and only one logon is required.
2. A pre boot environment will be used for authentication. Credentials will be used to authenticate the user in compliance with [complete as appropriate]password security policy. (*Some enterprises have a requirement to use two factor, and this should be reflected here as required)*.

Conclusion For Corporate Data Security Policies

In today's organizations, sensitive data is stored and accessed on a variety of mobile devices, including Secure drives. The storage capacity, size, low price and plug-and-play functionality are some of the reasons why their use has increased enormously. Secure drives are often handling corporate information, such as financial information, forms, employee documents and customer data. These mobile devices remain largely unprotected and uncontrolled by IT departments, leaving business susceptible to consequences which may be devastating such as lost reputation, jobs and profits.

Loss of company information is the result of employee ignorance about the risks associated with the use of Secure drives or their willingness to skirt policies in order to work more productively. Thus most of the actions are not intentional or malicious but accidental and unintended. Although there is increasing awareness of the risks and costs related to the insecure usage of Secure drives, there is still a significant amount of work to do. It is therefore crucial that IT asset managers prepare themselves and their organizations to regulate, manage and audit the use of Secure drives as ensuring the ability to secure information on the network and the opportunity to manage data which enter and leave the company environment is key for any organization regardless of its size and maturity.

With the increased number of portable devices used in business, with employees travelling and taking work home, a secure use of Secure drives and awareness of the related risks should be an

integral part of the organization's overall security strategy.

Reference of Corporate Data Security Policies

'Afghan market sells US military flash drives', Paul Watson, Los Angeles Times, *18 April 2006, available at http://www.veteransforcommonsense.org/ArticleID/7120 (last visited on 28 May 2008). 'Analysis of USB flash drives in a virtual environment', Derek Bem and Ewa Huebner,* Small ScaleDigital Device Forensics Journal, *Vol. 1, No 1, June 2007.*

'Another laptop stolen from Pfizer, employee information compromised', Lee Howard, 12 May 2008,available at http://attrition.org/dataloss/2008/05/pfizer01.html (last visited on 30 May 2008). 'Closed doors policy', Daniel Tynan, FedTech Magazine, *August 2007, available at http://fedtechmagazine.com/article.asp?item_id=352 (last visited on 30 May 2008).'Data breaches are "everyday incidents"', Matt Chapman, vnunet.com, 15 Nov 2007, available at http://www.vnunet.com/vnunet/news/2203540/security-breaches-everyday (last visited on 30May2008).*

'Data-leak security proves to be too hard to use', Infoworld.com, available at http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html (last visitedon 2 June 2008).

Dataquest insight: Secure drive market trends, worldwide, 2001–2010, *Joseph Unsworth, Gartner, 20 November 2006.*

DataTraveler for Enterprise, *Kingston, 2008, available at http://www.kingston.com/flash/DataTravelers_enterprise.asp (last visited on 30 May 2008).*
DataTraveler Secure *and* DataTraveler Secure — Privacy Edition White Paper, *KingstonTechnology,Rev. 2.0, June 2007.*
Determine the appropriate level of ITAM controls for mobile assets, *Jack Heine, Gartner, 15 November 2005. 'Disc listing foreign criminals lost for year',* The Times, *20 February 2008.*
Educational security incidents (ESI) — Sometimes the free flow of information is unintentional, *available at http://www.adamdodge.com/esi/month/2008/01*