Example
Tech Documentation

Information Classification Scheme

Updated: 2011.01.10 | Security classification: **UNCLASSIFIED**

Overview

All data handled by Example must be classified into one of four security levels, each of which requires different levels of protection. Employees must be able to identify the security classification of the data they work with. If there are questions as to the level of data classification, employees are required to obtain clarification from their management.

Security Levels

SECRET

Secret data requires strong security controls to prevent unauthorized access or modification of the data.

- Unauthorized access or disclosure of this level of data can result in significant financial losses and/or legal, regulatory, or reputation damage to Example.
- Card Holder Information (including PAN) is ALWAYS considered Secret and should be secured accordingly.

The two categories of Secret data recognized by Example are as follows:

Example Secret
This is data or information kept by Example that relates to its financials, business strategies, personnel data, legal matters, technical specifications, or other information that could significantly harm Example or its employees if it is not adequately protected.

Customer Secret
This is private information provided directly or indirectly by our customers that is necessary for fulfillment of services provided by Example. This includes private consumer information such as names, addresses, telephone numbers, etc., and account numbers, information about individual accounts, or any other information that can be individually tracked to a consumer. Various federal and state consumer and privacy laws specify the type of protection required for this information as well as legal agreements with third parties such as credit card issuers, banks, etc. Various federal and state laws, as well as legal agreements with third parties, may dictate the type of protection required for this information.

CONFIDENTIAL

Confidential information is intended for internal use within Example, but is not intended for general disclosure to the public. Accidental or malicious disclosure of Confidential information to unauthorized parties may require a response from Example, but significant damage to the brand of Example or other losses will not result.

PUBLIC

Public information is intended to be shared with any individual outside Example. This includes information included on Example's web site made available to unauthenticated users, marketing materials, general Example information, etc.

UNCLASSIFIED

If your document does not fit into either of these 3 preceding security levels, mark it as "Unclassified". This will likely be most of the documents you create. If a document is not explicitly marked with a classification or as "unclassified", it will be assumed to be for consumption within Example and with Example's partners on a need to know basis.

Data Protection Policies

Secret information is to be secured and protected while in transit over networks and while in storage.

Secret Data in Transit

The following table lists the minimum level of security controls required to protect Secret data while it is in transit over computer networks. Additional security controls may be necessary for a given application or data based upon business risk, regulations, environmental factors, etc.

Network type	**Encryption requirements for data in transit**
Internet	All Customer and Example Business Secret data must be encrypted in transit over the Internet. Note: The Internet is used for many types of communications in addition to web browsing. Examples of typical Internet traffic are: • Email sent and received to external email addresses • Instant Messaging • Web collaboration and workflow tools • Video and audio streams
Private telecom networks (wide area networks, MPLS, point-to-point networks, etc.)	All Customer Secret data must be encrypted during transport over private wide area networks, unless a written exception is granted by the security@Example.
Wireless networks	All Customer and Example Business Secret data must be encrypted in transit over wireless networks using a method approved by security@Example.
Private local area wired networks (e.g., office Ethernet networks)	Wherever possible, internal data flows containing Secret information should be protected using transport or end-to-end encryption techniques.
Extranets (networks managed by our business partners)	The security@Example must be contacted to evaluate requirements for encryption of data in transit over Extranets.

Secret Data in Storage

The requirements to encrypt Secret data stored on electronic media vary depending on the sensitivity of the data and how the data is accessed/used. The following are the minimum level requirements to protect Secret data in storage.

Data type and use	Requirements to encrypt data in storage
Passwords (or "pass–phrases") to access applications that contain Secret data, or passwords required to access/decrypt data that is stored encrypted.	Passwords must be stored encrypted or hashed.
Credit card, debit card, or bank account numbers stored on production servers within a secured data center or in security@Example-approved third party data centers.	Must be stored encrypted.
Non–account Customer Secret data stored on production servers within secured Example data centers or security@Example–approved third party data centers. Examples: addresses, birth dates, driver's license, etc.)	Should be stored encrypted where possible.
Customer Secret data stored on laptops, office desktop computers, removable media such as USB drives, compact flash memory cards, CD/DVD media, etc.	**NOT PERMITTED** unless approved by security@Example in writing.
Customer Secret data stored on servers secured within Example office locations.	Must be encrypted or security@Example must authorize unencrypted storage based upon the presence of compensating controls.
Customer Secret data stored on security@Example–approved and controlled backup media used for disaster recovery or business continuity purposes.	Must be encrypted, media must be labeled Secret and must be physically secured at all times. Transport of such media outside of secured Example facilities must be done via a method approved by the security@Example.

Data Protection Standards

The current Standard for encrypting secret data is Winzip.

- Files that will be shared over email, file sharing services (e.g., Dropbox), or removable media must be encrypted (password protected).
- The encrypted file and the associated encryption/decryption password must be transmitted to the receiving party over *two separate communication channels*, e.g.,
    - The file being shared via Drop-box; and
    - The decryption password sent via SMS/Text Messaging.

Non-electronic Data Protection (paper reports, documents, etc.)

Employees must label all documents that are Secret:

- By using a standard format in page footers, or
- By stamping each page clearly with a warning.

All reports that contain Customer Secret data must always be physically secured at Example facilities, and must not leave the premises unless they are reports intended for distribution via authorized delivery channels approved by management.

Employees must exercise care in protecting Example Business Secret documents when carrying them out of the facility or using them at home or elsewhere. During travel, Example Business Secret documents should be transported as carry–on baggage and should be kept in hotel–provided safes when possible.

Secret information on paper must be shredded before disposal or placed in secured bins for bulk shredding. Bins for waste paper containing Secret information are placed throughout Example facilities.

Servicing of Equipment Containing Secret Data

When a computer requires service by non–Example technicians, it must be shut down prior to servicing to prevent access to temporary files maintained by the operating system.

Copiers, printers, and other multi–function devices may contain disc drives or other storage media that retain images of every scanned, faxed, and printed document they process.

- These images are often retained in an unencrypted file, usually until all available space is used.
- These storage media must be removed and the media completely wiped or destroyed prior to removing the devices from Example premises.

When disposing of obsolete computer equipment, ensure that the hard discs are completely wiped of Secret data and software. The software used for erasing secret data must be approved by security@Example.

Protection of Confidential and Public Data

Data intended for public access does not require any security controls; although access to data may be tracked for valid business purposes and in accordance with our published Privacy Policy.

Confidential data requires a basic level of authentication to establish that the user is a current employee of Example. This may be the possession of a badge to gain access to a Example facility, or via remote network access provided via an approved authentication mechanism. Additional levels of authorization may be required to establish membership in a group or role to limit access to Confidential information based upon job function or responsibility as required by management.