Information Sensitivity Policy

April 2016

Table of Contents

PURPOSE

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non employees, as well as the relative sensitivity of information that should not be disclosed outside of YourCause, LLC ("YourCause") without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines, as well as to emphasize common sense steps that employees shall take to protect YourCause Confidential information (e.g., YourCause Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Please either refer to the YourCause Data Classification Policy or consult your manager for any questions about the proper classification of a specific piece of data. If ever in doubt as to the proper classification of data, employees shall always assume such data to be confidential by default.

SCOPE

All YourCause information is categorized into four main classifications:

- YourCause Sensitive and Confidential Data
- YourCause Restricted Data
- YourCause Internal Data
- YourCause Public Data

YourCause Sensitive and Confidential Data is any information protected by federal, state or local laws and regulations or industry standards such as the Texas State Data Breach Notification Act, similar state laws and PCI-DSS. This classification applies to the most sensitive business information that is intended for use strictly within YourCause.

YourCause Restricted Data is any information that is contractually protected as confidential by law or contract, as well as any other information that is considered by YourCause to be appropriate for confidential treatment. Its unauthorized disclosure could adversely impact YourCause or its customers, suppliers, business partners, or employees.

YourCause Internal Data is internal operating procedures, manuals, memos, emails, as well as sensitive financial and technical information that is proprietary or produced only for use by members of YourCause and who have legitimate purposes to access such data.

YourCause Public Data is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to YourCause, LLC. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

While YourCause information is codified into four distinct classifications, these data reside within two major categories:

- YourCause Privileged or Confidential Information
- YourCause Public Information

YourCause Privileged or Confidential Information embodies YourCause sensitive, restricted and internal data. It is a continuum in that some information is more sensitive than other information, and should be protected in a more secure manner.

YourCause Public Information is all information that is otherwise not codified as part of YourCause sensitive data, restricted data or internal data. As a rule, any data rated as public may be distributed and accessed by anyone without prior approval from YourCause management or information security team.

YourCause personnel are encouraged to use common sense judgment in securing YourCause Privileged or Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager.

POLICY

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as YourCause Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the YourCause Confidential information in question.

Below are guidelines indicating the manner in which sensitive data in hardcopy and/or electronic form shall be handled based upon the data sensitivity. Markings stipulating the owner and nature of the data *("3rd Party Privileged or Confidential")* may be used to annotate any sensitive document.

i. Minimal Sensitivity

Data of minimal sensitivity is comprised of general corporate information and some personnel and technical information.

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "YourCause Privileged or Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "YourCause Proprietary" or similar labels at the discretion of the individual business unit or department. Even if no marking is present, YourCause information is presumed to be "YourCause Privileged or Confidential" unless expressly determined to be YourCause Public information by a YourCause employee with authority to do so.

Access: YourCause employees, contractors, or people within a business on a need-to-know basis.

Distribution within YourCause: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of YourCause internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it shall be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Dispose outdated paper information in specially marked disposal bins on YourCause premises. Electronic data should be expunged/cleared. Media shall be reliably erased or physically destroyed.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

ii. More Sensitive

Data of more sensitivity is comprised of business, financial, technical, and personnel information.

As the sensitivity level of the information increases, you may, in addition or instead of marking the information "YourCause Privileged or Confidential" or "YourCause Proprietary", wish to label the information "YourCause Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. Marking is discretionary at all times.

Access: YourCause employees and non---employees with signed non-disclosure agreements that have a business need to know.

Distribution within YourCause: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of YourCause internal mail: Sent via U.S. mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within YourCause, but should be encrypted or sent via a private link to approved recipients outside of YourCause premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: Such information shall be disposed in specially marked disposal bins on YourCause premises. Electronic data shall be be expunged/cleared. Media shall be reliably erased or physically destroyed.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

iii. Most Sensitive

Data of most sensitivity is comprised of trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of YourCause.

To indicate that YourCause Confidential information is very sensitive, you shall label the information "YourCause Internal: Registered and Restricted", "YourCause Eyes Only", "YourCause Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of YourCause Privileged or Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (YourCause employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within YourCause: Must be directly delivered. Signature is required, and envelopes shall be stamped confidential or approved electronic file transmission methods shall be used.

Distribution outside of YourCause internal mail: Must be directly delivered. Signature is required and approved private carriers shall be used.

Electronic distribution: No restrictions to approved recipients within YourCause, but it is highly recommended that all information be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information shall be stored in a physically secured computer.

Disposal/Destruction: Such information shall be disposed of in specially marked disposal bins on YourCause premises. Electronic data shall be expunged/cleared. Media shall be reliably erased or physically destroyed.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, legal action, and/or termination of employment.

Definitions

Appropriate measures

In order to minimize risk to YourCause from an outside business connection, the use of YourCause computers by competitors and unauthorized personnel must be

restricted so that, in the event of an attempt to access YourCause corporate information, the amount of information at risk is minimized.

Configuration of YourCause to other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Retrieve all mails from mail slots and coordinate such requirements with the CFO.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelops Stamped "Confidential"

No special envelope is required. Document(s) shall be inserted into an interoffice envelope, sealed, addressed, and stamped as "*confidential*".

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. In the case a different mailer needs to be used for business purposes, the appropriate support organization shall be contacted..

Approved Encrypted Email and Files

Techniques include the use of AES and PGP. AES encryption is available via many different public domain packages on all platforms. PGP use within YourCause is done via a license. Electronic mail encryption is achieved via an enforcement of a TLS connection between the two parties with the use of AES algorithms to encrypt the email content. Please contact the appropriate support organization if you require a license.

Company Information System Resources

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC or Mac, a separate program supplied by Norton Utilities must be used to overwrite data. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On Mac’s and PC's, this includes using passwords on screensavers.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of YourCause.

Encryption

Secure YourCause Sensitive information. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or Chief Information Officer for further guidance.

One-Time Password Authentication

One-Time Password Authentication on Internet connections is accomplished by using one-time password tokens to connect to YourCause's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never

leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Confirmation of Receipt and Agreement

I have received, read, understood and am in agreement with the YourCause, LLC Information Sensitivity Policy updated on the 1st day of April 2016.

Date Recipient's Signature

Date Manager's Signature