Microsoft Confidential
Simple Acts to Prevent Leaks

Module 1: Confidentiality

Where can you find the Microsoft Confidential course SharePoint site?

http://lcaweb/policies/Confidential/Pages/ConfidentialTraining.aspx

What can you do to maintain confidentiality?

- Read and follow the Microsoft Confidential Information Policy.
- If you have questions, ask your LCA representative about how to identify and protect confidential information.
- Report actual or potential leaks immediately.
- Talk to your peers and manager if you see an opportunity to improve confidentiality practices.

How can you respond to and report an incident?

- If you become aware that confidential information has been disclosed improperly, or has leaked, it is important to act quickly so that the appropriate people can take steps to mitigate the potential impact.
- If you know — or think you know — about a potential or actual incident, report it to your manager, go to Report-It-Now, or follow the security incident process for your team.

Module 2: Protecting Physical Assets

Protect building access through these simple acts.

- Remember: One Card, One Entry.
- Do not let people tailgate through a secure door.
- If you see someone tailgating, politely ask the person to swipe his or her badge.
- Always escort visitors.
- Be sure to close secure doors behind you.

Looking for more details about protecting physical assets?

BitLocker FAQ

BitLocker Selection Guide

Disposing of Hardware

Physical Access Control

Protecting Your Data with Windows 8.x BitLocker

Securing Your Computer

Securing Your Windows Phone

Securing Your Windows RT Companion Device

Theft Prevention

Visitors

Protect workspaces through these simple acts.

Meetings

- Remind attendees that the meeting is confidential.
- Send a link to a secured location instead of attaching a file or including confidential information in the body of the meeting invitation, because it may be accessible to receptionists, calendar delegates, or others who do not need to know.
- Use nonspecific subject lines for meeting requests so that confidential information is not exposed to calendar delegates or on conference room displays.
- If the meeting includes remote attendees through Microsoft Lync, Skype, Microsoft Live Meeting, and so forth, ask participants to identify themselves and make certain you can see when attendees join the call.

Whiteboards

- Erase whiteboards at the end of each meeting.
- When you take photos of whiteboards:
  - Make certain you have disabled the "auto upload to cloud storage" feature on your phone or properly secured your cloud folder.
  - Use the Snap function in the Campus Experience application for your Windows Phone.
  - Do not enable auto upload to Microsoft OneDrive.

Documents

- Watermark confidential documents with "Microsoft Confidential."
- Print out hard copies for meetings only as needed.
- Dispose of confidential documents using the shredding bins available in supply rooms.
- Collect copies of confidential documents at the end of the meeting.
- Store printouts where they cannot be stolen.

Work area

- Lock your computer when it is unattended.
- Keep hard drives, confidential documents, samples, and prototypes in locked storage.
- Ensure that confidential information and assets, such as prerelease hardware and whiteboards, are not visible through windows.

Protect hardware through these simple acts.

Configure

- Install BitLocker and BitLocker-to-Go on your devices.
- Encrypt or password-protect your mobile devices.
- Enable functionality to remote-wipe your mobile device if it is lost or stolen.

Protect

- Do not let anyone take photos of confidential hardware.
- Make certain that company assets, especially prototypes and prerelease hardware, are secured and stored in approved locations.
- If you have to transport prototypes or prerelease hardware, find out whether you need a security escort.
- Transport prototypes or prerelease hardware in a nondescript box or bag to prevent others from seeing it.
- Properly dispose of or recycle hardware according to policy.
- Notify Security if your hardware is lost or stolen.

Module 3: Securing Data

Secure data when using email through these simple acts.

Securing data

- Send a link to a secure location instead of attaching a file.
- Use Information Rights Management (IRM) to prevent information from being printed, forwarded, or copied.
- If you cannot apply IRM protection, use password protection or encryption.

Securing user access

- Send confidential information only to those who need to know.
- Use project-specific, mail-enabled security groups or distribution groups.
- Expand distribution groups to make certain it is appropriate to disclose the information to all the members.
- Use the Delay Delivery feature in Outlook to allow you time to stop an email sent to an unintended recipient.
- Disable the Auto-Complete List feature in Outlook when you are working on confidential projects.

Secure data when using Microsoft SharePoint through these simple acts.

Permissions and security groups

- Whenever possible, use RAMWEB security groups to automatically manage expiration and revoke access based on organizational changes.
  - If your team does not use RAMWEB for access, you can manage security groups through Forefront Identity Management or IDWeb.
- Routinely review user access lists and security group memberships used to provide access to sites you manage.
- Only grant site permissions to users who need the information to do their job.
- Disable external sharing functionality to sites containing confidential information.

Credentials

Safeguard your corporate credentials.

- Never share your corporate credentials with anyone.
- Use unique credentials (not your corporate email address and password combination) for third party applications and websites.
- Remember that external sites, such as O365, can be accessed with your credentials. They do not require a smartcard.

Information Rights Management (IRM)

- Use IRM on document libraries to protect confidential documents.
- Create separate libraries for confidential and nonconfidential information.
- Create separate libraries for files that cannot be rights-managed, such as PDFs and media files, and password protect the files.

Secure data on cloud-based storage and services through these simple acts.

- Be aware of who has access to your folders on cloud-based storage and services such as Microsoft OneDrive, Google+, Dropbox, OneNote, iCloud, and Evernote.
- Do not sync folders to unsecured devices such as your home computer.
- Before you post anything, clearly understand whether your group restricts the use of OneDrive or other cloud-based storage and services.
- Cloud storage technology is changing quickly. To stay current on best practices, go to ITWeb Support.
- Do not use personal cloud storage for business purposes. Instead, use OneDrive for Business.

Looking for more details about securing data?

General and email

IDWeb

IDWeb How To

Successful Meetings with Lync 2013

Work Smart: Managing Email

Work Smart: Securing Business Information

SharePoint

Information Classification Wizard

ITWeb: SharePoint Services

RAMWEB

Cloud-based storage and services

Access Files from Any Windows 8.1 Device with Work Folders

ITWeb Support

OneDrive for Business

Save and Share Documents in the Cloud with OneDrive Pro

Prevent disclosure in public locations through these simple acts.

Consider the location

- Be careful when discussing confidential information in Microsoft public areas such as hallways, elevators, restrooms, cafeterias, the Commons, shuttles, and the Connector.
- Be careful when discussing work in public places such as restaurants, athletic clubs, airports, and taxis.
- Be aware that connecting to unsecured Wi-Fi networks may expose data you send or receive.

Consider the person you are talking with

- Do not share any Microsoft confidential information with Microsoft employees who do not have a need to know.
- Do not share any Microsoft confidential information with friends, family members, or former Microsoft colleagues.
- Do not share any Microsoft confidential information with event attendees or speakers.
- Do not talk to reporters or bloggers without authorization from public relations.

Consider the confidential materials

- Be careful when you work with documents (on hard copy or on your devices) that contain Microsoft confidential information in public places.
- Do not leave confidential materials (such as software, hardware, and specifications) unattended or unlocked at home or in your vehicle.
- Ensure public presentations do not include confidential information. If you have questions or are not certain, contact LCA.

Prevent disclosure when using social media through these simple acts.

- Follow the Guidelines for Engaging with Social Media.
- Do not blog, tweet, or post confidential information on social networking sites.
- Do not post information about confidential projects, including project names, in job descriptions or on professional networking sites such as LinkedIn.
- Make your Microsoft affiliation clear when blogging, tweeting, or posting about Microsoft or the technology industry.
- If the confidential information cannot be shared with the entire company, do not post it on internal sites that are broadly accessible, such as Yammer or Dr. Whom.
- Do not comment on rumors or speculation, especially on leaked information. Your comments can be misrepresented, fueling additional rumors or leaks.

Looking for more details about preventing public disclosure?

Ask the bloggers alias or email lcablogg

Blogging Best Practices

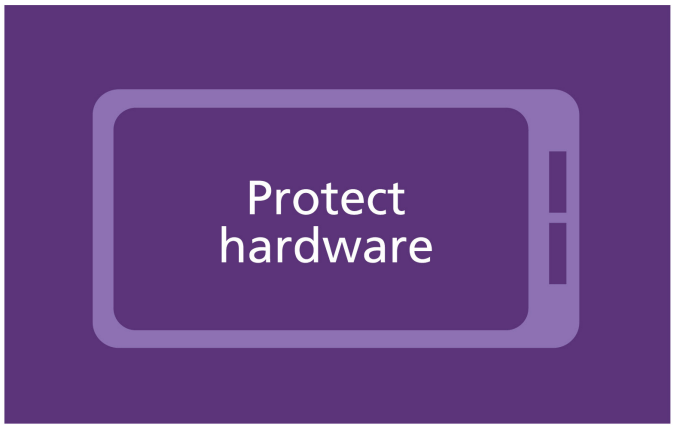
Guidelines for Engaging with Social Media

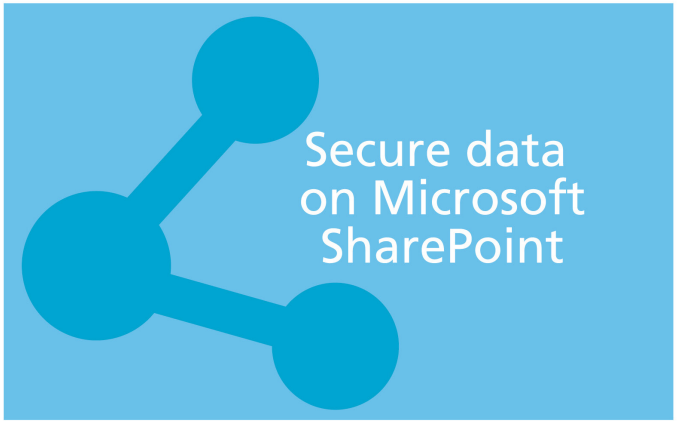
LCA Blogging and Social Media Guidelines

Microblogging Accounts like Twitter

Social Engineering

Social Media FAQ





http://lcaweb/policies/Confidential/Pages/ConfidentialTraining.aspx