This course provides suppliers important information about the Microsoft Supplier Code of Conduct.

A number of topics from the Code are covered. Each topic begins with an explanation, followed by scenarios and questions. At the conclusion of the topics are key learning points.

**The Code, Suppliers, and this Course**

In this training, the Supplier Code of Conduct is referred to as "the Code." “Supplier” refers to the company providing the service. “External Staff” refers to Supplier employees working on behalf of Microsoft. “Microsoft sponsor/contact” refers to the Microsoft full-time employee who is the External Staff member’s primary contact.

Microsoft expects Suppliers and External Staff to act ethically and with integrity. This commitment to integrity is expressed in the Supplier Code of Conduct.

**Doing Business with Microsoft**

In order to do business with Microsoft, Suppliers are required to embrace ethical business practices and conduct business in compliance with all regulations, laws, and applicable supplier contracts and policies.

Suppliers demonstrate this commitment by complying with the Code and training their employees on the Code.
If you wish to report questionable behavior or a possible violation of the Supplier Code of Conduct, please contact Microsoft through any of the following methods:

**Call:**
In the U.S.: 1-877-320-MSFT (6738)
Outside the U.S. (collect): 1-470-219-7087

**Email:** [Business Conduct and Compliance alias](mailto:Business.Conduct.Compliance@microsoft.com)

**Online:** [Microsoft Integrity Website](https://www.microsoft.com/en-us/about/useresponsibility)

**Mail:**
Microsoft Corporation
Corporate, External, and Legal Affairs (CELA) group
One Microsoft Way
Redmond, WA 98052

**Fax:** 1-425-708-7177

Microsoft will maintain confidentiality to the extent possible and will not tolerate any retribution or retaliation taken against any individual who has, in good faith, sought out advice or reported questionable behavior or a possible violation of this Supplier Code of Conduct.
# Introduction

## Executive Welcome – Amy Hood

Hello. I’m Amy Hood, Chief Financial Officer at Microsoft.

This is an important time for Microsoft and for our suppliers. We have great opportunities ahead, and we rely on great Suppliers to help us succeed. To be successful, we must continue to earn and maintain the trust of customers, partners, and governments. We build trust everyday by living our values and by acting with honesty and integrity.

As an important part of the Microsoft team, suppliers must live by high standards of ethics and integrity. That’s why we’ve developed this course on the Microsoft Supplier Code of Conduct, which highlights issues you need to know in order to comply with the Code and adhere to our culture of ethical conduct.

Unethical and untrustworthy companies do not succeed. A momentary lapse in judgment by a single Microsoft Supplier has the potential to erode the value and the trust we bring to customers.

Help us seize our opportunities by doing the right things in the right way.

Thanks for your commitment to our business and for your close attention to this course.
The Supplier Code of Conduct

The Code describes Microsoft’s standards for ethical business practices and regulatory compliance.

This Course contains scenarios, questions, and key learning points about various parts of the Code, but not all parts of the Code. Therefore, please fully review each section of the Code, including:

- Compliance with the Supplier Code of Conduct
- Legal and Regulatory Compliance Practices
- Business Practices and Ethics
- Labor Practices and Human Rights
- Health and Safety
- Environmental Regulations and Protection
- Protection of Assets and Intellectual Property
- Reporting Questionable Behavior

You may download the Code here:


Compliance with the Supplier Code of Conduct

Inform Microsoft

Suppliers and External Staff members must promptly inform their Microsoft sponsor/contact (or a member of Microsoft management) when any situation develops that causes an External Staff member to operate in violation of the Code. Use the reporting resources provided in the Code and described at the end of this Course.

Self-Monitor

External Staff members are expected to self-monitor and demonstrate their compliance with the Code.
Removal

Microsoft may require the immediate removal of any External Staff member who behaves in a manner that is unlawful or inconsistent with this Code or any Microsoft policy.

Section: Legal and Regulatory Compliance Practices

Section Introduction

Suppliers must conduct their business activities in full compliance with applicable laws and regulations while conducting business with or on behalf of Microsoft.

Important areas of compliance described in this section of the Code include:

- Trade
- Antitrust
- Boycotts
- Anti-Corruption
- Accessibility

In this section, we will focus on the Code’s prohibition of corruption and the Code’s requirements related to creating accessible products and services—but please be sure to familiarize yourself with the Code’s content on Trade, Antitrust, and Boycotts as well.
Topic: Anti-Corruption

External Staff members are prohibited from promising, offering, or paying a bribe to anyone.

**What does this mean?**
- External Staff members may not participate in bribes or kickbacks of any kind.
- This prohibition applies to dealings with both government officials, and individuals in the private sector.

**What is a bribe?**
- A bribe is any payment or offer of anything of value to an individual for the purpose of obtaining an improper benefit.
- This means that anything of value—such as cash, gifts, travel, loans, charitable donations, or job opportunities—may constitute a bribe under certain circumstances.

No External Staff member will suffer adverse consequences for refusing to pay or take a bribe, even if this results in the loss of business to Microsoft.

---

**Scenario: “A Suspicious Request”**

*In this scenario, Microsoft has hired a Supplier to secure a permit from a government agency. An External Staff member named Lia is dealing with an employee of the government agency named Mr. Smith, who is in charge of issuing the permits.*

**Lia, External Staff:** Thank you, Mr. Smith, for taking the time to discuss this request with me personally. I have not had any success getting this permit approved through the usual process.

**Mr. Smith, government employee:** Sometimes, it can be difficult to get a permit approved, because we are under-staffed and have a lot of work to do. How can I help you?

**Lia, External Staff:** I filed Microsoft’s application for a permit six months ago, but there has been no action. What can I do to get the permit approved?

**Mr. Smith, Government Employee:** I suggest you pay me for my time to look into this matter. The next time you are in the office, come and see me. I will make sure the
<table>
<thead>
<tr>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>What should Lia do?</td>
</tr>
<tr>
<td><em>Select all that apply.</em></td>
</tr>
<tr>
<td>A. Give the government employee cash to obtain the permit. The permit is important to Microsoft, so she should do what is necessary.</td>
</tr>
<tr>
<td>B. Report the official's request to her own manager and seek guidance.</td>
</tr>
<tr>
<td>C. Report the request to her Microsoft sponsor/contact and seek guidance, using the reporting resources described in the Code.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>The correct answer is both B and C, for these reasons:</td>
</tr>
<tr>
<td>- The request for an extra payment is suspicious and might be a request for a bribe.</td>
</tr>
<tr>
<td>- External Staff members must not pay anything of value to improperly influence any act or decision of any government employee.</td>
</tr>
<tr>
<td>Lia should not make any offers, promises, or payments to the government employee.</td>
</tr>
<tr>
<td>She should report the request both to her own (Supplier) manager and to her Microsoft sponsor/contact and seek guidance on what to do next.</td>
</tr>
</tbody>
</table>
Key Learning Points

- Microsoft prohibits corruption of government officials and the payments of bribes or kickbacks of any kind, whether in dealings with public officials or individuals in the private sector.

- Never promise, offer, or pay a bribe, directly or indirectly, in any form. Do not further Microsoft’s business interests in any improper or unlawful manner.

- Microsoft’s prohibition against bribes and kickbacks includes offering, promising, or paying anything of value (such as cash, gifts, travel, hospitality, loans, donations, job opportunities, or other benefits) for any improper purpose.

- Be alert and identify suspicious requests that may signify a heightened risk of corruption.

- Report suspicious requests or activity both to the Supplier and to the Microsoft sponsor/contact and seek guidance on what to do next.

- Use the reporting resources provided in the Code and described at the end of this course.

- Read what the Code says about anti-corruption.

Topic: Accessibility

Topic Introduction: Accessibility

More than one billion people in the world live with a disability. Accessibility is about making sure all people, regardless of ability, have equal access to physical and electronic environments and resources.

Microsoft’s mission is to empower every person and every organization on the planet to achieve more—and creating products and services that are accessible to people with disabilities is an important part of that.

Some people with disabilities use assistive technology such as screen readers, screen magnifiers, and speech recognition tools. We need to test to ensure that our products and services offer great experiences to people when they are using assistive technology.

When Microsoft Suppliers create website deliverables or do work contributing to Microsoft products, they are responsible for complying with Microsoft’s accessibility
Cindy is an External Staff member employed by a new Microsoft Supplier. She understands that Microsoft has accessibility requirements, but she isn’t sure which of her company’s deliverables need to be accessible.

Select all types of deliverables below which should be accessible.

A. Word and PowerPoint files
B. Web sites
C. Videos
D. Applications

Accessibility requirements apply to all of these deliverable formats.

Microsoft has many accessibility resources to help you ensure your deliverables are accessible.

Follow these tips to create accessible files, websites, and applications:

- Learn the Microsoft Accessibility Standards (MAS) and how best to meet them.
- Follow the guidance provided by Microsoft’s many accessibility resources.
- Make sure all videos have closed captions and, when necessary,
audio descriptions.
- Make sure colors meet at least a 4.5:1 contrast ratio.
- Add objective alternative text (or alt text) to all images.
- Use meaningful link text: link the text that actually says what you are linking to, rather than something like “click here” or “learn more”.
- Test your deliverables with assistive technologies.

- Follow these etiquette guidelines when interacting with a person who has a disability:
  - When speaking with a person who has a disability, look at them and speak directly to them, even if the person is blind or working with an interpreter.
  - Use positive, people-first language when referring to people with disabilities.
  - Never touch assistive tools such as wheelchairs, guide dogs, canes, or phones.
  - If a person has low vision or is blind, announce yourself when you walk by or enter a meeting so that they can easily know who is there.

- Read what the Code says about accessibility.

### Accessibility Resources

Microsoft has many accessibility resources to help you ensure your deliverables are accessible.

- Accessibility Subject Matter Experts at Microsoft can provide you with guidance and help. You can find contact information for Subject Matter Experts on CorpNet or ask your Microsoft Representative to connect you with them.
- The Accessibility Learning Program Library has training materials to help people understand and implement accessibility. (Requires Microsoft CorpNet access.)
- The Microsoft Accessibility homepage offers the latest information around our products and services.
- The Office Accessibility Center offers checklists and tutorials to help you author
Section: Business Practices and Ethics

Section Introduction

External Staff members must conduct their business interactions and activities with integrity. Important areas of compliance described in this section of the Code include:

- Business Records
- Speaking to the Press
- Gift Giving
- Conflicts of Interest
- Insider Trading

Let's learn more about business records, gifts, and conflicts of interest.

Topic: Business Records

Topic Introduction: Business Records

External Staff members must honestly and accurately record and report business information in contracts, purchase orders, invoices, and any other records.

External Staff members play an important role in ensuring that business information is accurate, complete, and transparent.

Actions that External Staff members can take to ensure compliance with these requirements include:

- Make sure all contract documents are complete and signed before beginning work on a project.
- Accurately document project changes in an amended Statement of Work ("SOW"), Purchase Order ("PO"), or Change Order.
- Invoice Microsoft only for work actually completed that meets the requirements of the contract documents.
- Return any mistaken payments or overpayments from Microsoft immediately.
- Seek clarification of changed deliverables and refuse any request that might violate the Code.

Scenario: “Lack of Transparency”

_In this scenario, an External Staff member named June is launching a marketing event for Microsoft customers. Her Microsoft contact is Marcus, a marketing manager._

_June, External Staff:_ Marcus, we are ready for the customer conference. The presentations have been finalized, and we have a nice welcome package for each customer.

_Marcus, Microsoft employee:_ Thanks. Listen, there are some customers attending who are considering important deals. I want you to help close these deals.

_June:_ OK! What should I do?

_Marcus:_ Microsoft hired you for your marketing expertise. Just do whatever it takes to show the customers why they should purchase Microsoft products.

_[Two weeks have gone by, and the event is over]._

_Marcus:_ June, I am in trouble with my manager at Microsoft! He told me that you paid for customers to go on a ski trip after the conference. Then you invoiced Microsoft for “design services” to hide the trip expenses!

_June:_ But you told me to do whatever it takes! A customer suggested the trip. The Statement of Work did not cover this, so I put the trip expenses under design services.
## Question

**Did June violate the Code?**

*Select the correct answer.*

A. Yes. June’s invoice was inaccurate and deceptive.

B. No. External Staff members are expected to comply with the instructions of their Microsoft sponsor/contact.

## Answer

A is the correct answer. June made several mistakes:

- She did not describe the services truthfully in the invoice.
- She did not seek clarification from the Microsoft contact on the services required and did not revise the Statement of Work to include those services.
- She may have violated the policies of the customer and Microsoft by arranging a ski trip without advance approval.

## Key Learning Points

- Always seek clarification from your Microsoft sponsor/contact on the services required, document the changes appropriately, and make sure the request does not violate the Code.
- Never provide or facilitate services that might be improper, even if a Microsoft employee makes the request.
- Unless it has been authorized and approved in writing by Microsoft, suppliers are prohibited from paying expenses for travel, lodging, gifts, hospitality, or charitable contributions for government officials on Microsoft’s behalf.
- Do not conceal or misrepresent services performed for Microsoft. Accurate and transparent documentation of all services is important.
Read what the [Code](#) says about business records.

## Topic: Gifts, Travel, and Hospitality

### Topic Introduction: Gifts, Travel, and Hospitality

External Staff members should use caution before giving anything of value to a Microsoft employee. Microsoft prohibits any gift that is intended to or might appear to influence or obligate the recipient, or compromise the recipient’s judgment.

**What is a Gift?**

A gift is anything of value offered to a Microsoft employee, such as:

- Travel and lodging;
- Hospitality (meals and entertainment);
- Excursions such as cruises, golfing, and spa visits;
- Prizes from raffles, sweepstakes, or contests;
- Tickets to events.

**Are certain kinds of gifts always prohibited?**

Yes—the following gifts are prohibited in all cases, regardless of amount or circumstance:

- Gifts of money or cash equivalents, such as gift certificates and gift cards.
- Gifts to any member of the Global Procurement Group (GPG) or its representatives.
- Gifts with an improper purpose.
- Gifts that violate the gift policies that apply to Microsoft employees.

Microsoft requires that External Staff members exercise good judgment and understand policy limits when considering gifts to Microsoft employees. Even a well-intentioned gift might compromise the recipient’s judgment, or otherwise create a conflict of interest.
Scenario: “Supplier Summit”

In this scenario, an External Staff member named Richard wishes to invite a Microsoft employee named Chris to a supplier conference.

Chris, Microsoft employee: Hi, Richard. I understand your company is sponsoring the Global Supplier Summit in Florida.

Richard, External Staff: Yes, we are very excited about it. Hundreds of companies are attending.

Chris, Microsoft employee: Sounds interesting.

Richard, External Staff: The conference is a great opportunity for Microsoft to present its product roadmap. I hope you and your team can be my guests at the conference. We will have a lot of fun together.

Chris: Our budgets are limited this year. What’s involved?

Richard: Don’t worry. We will provide travel and lodging for your team. We offer a fishing trip and spa treatments as well.

Question

Should Richard make this offer?

Select the correct answer:

A. Yes. The offer is clearly for a legitimate business purpose and mutually beneficial for both companies.

B. No. Richard should first determine if Microsoft employees may accept travel, lodging, and gifts from suppliers.

C. Yes. The offer is appropriate because Richard is letting Microsoft choose which employees will attend.
Answer

The correct answer is B.

Richard should exercise due diligence to determine if the offer violates Microsoft policy.

In addition, the spa treatments and fishing trip do not appear to have a legitimate business purpose.

---

Key Learning Points

- Review the Code and ask your Microsoft sponsor/contact or the recipient what the limits are before offering anything.
- Never provide a gift of money or cash equivalent such as a gift card or gift certificate.
- Improper gift giving may result in the termination of a Supplier contract and/or disciplinary action for the Microsoft employee.
- Read what the [Code](#) says about gifts.

---

Topic: Conflicts of Interest

Topic Introduction: Conflicts of Interest

External Staff members must avoid conflicts of interest as well as the appearance of conflicts when performing work for Microsoft or representing Microsoft.

**What are examples of Supplier conflicts of interest?**

- A conflict of interest arises when a Supplier or External Staff member attempts to influence a Microsoft decision of action that is not in the best interest of Microsoft.
- In the course of negotiating an agreement with Microsoft, External Staff members may not negotiate directly with any of their family members who are employed by Microsoft.
- While performing work or providing services for Microsoft, External Staff members
may not deal directly with any of their family members who are employed by Microsoft.

- If a Microsoft employee (or the Microsoft employee’s family member) holds a significant financial interest in a Supplier, then the Supplier may not deal directly with the Microsoft employee.

### Scenario: “Dealing with a Spouse”

*In this scenario, two External Staff members are discussing how to respond to a Microsoft Request for Proposal (“RFP”).*

**Susan, External Staff:** Bill, can you help me respond to Microsoft’s RFP? We need to win this contract. It is very important to our company.

**Bill, External Staff:** Yes, what can I do to help?

**Susan:** I believe your spouse is an employee of Microsoft?

**Bill:** Yes, she is. I think she might be working on this project, actually.

**Susan:** Great! I want you to find out all you can about the RFP from her, and get her feedback on our proposal. Your relationship can really help us win this contract.

### Question

**How should Bill respond to Susan’s request?**

*Select the correct answer.*

A. Bill should talk to his spouse and try to find out as much information as he can about the project. This will help the Supplier make a strong proposal, which is in the best interests of Microsoft.

B. It is improper to seek Microsoft’s internal information about the RFP to gain an advantage. Bill should decline Susan’s request. However, Bill may ask his spouse to recommend the Supplier to the Microsoft decision makers on the RFP.

C. It is a conflict of interest for Bill to deal directly with his spouse on this project. Bill should not work on this project.
**Answer**

C is the correct answer.

It is a conflict of interest for an External Staff member to deal directly with a family member employed by Microsoft. Susan should not have made the request of Bill.

Direct dealing with a spouse employed by Microsoft could result in an unfair advantage for the Supplier and harm the best interests of Microsoft.

B is partially correct. It is improper to seek Microsoft's internal information about the RFP to gain an advantage, and Bill should decline Susan's request. However, Bill should not ask his spouse to recommend the Supplier to the Microsoft decision makers.

<table>
<thead>
<tr>
<th><strong>Key Learning Points</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ An External Staff member who has a family member employed by Microsoft should take steps to ensure that there are no direct dealings with the family member.</td>
</tr>
<tr>
<td>▪ These steps may include notifying the Supplier of the conflict of interest, avoiding any work with the family member, and notifying Microsoft of the relationship.</td>
</tr>
<tr>
<td>▪ An External Staff member who has a family member employed by Microsoft should also avoid asking the family member to recommend the Supplier to Microsoft.</td>
</tr>
<tr>
<td>▪ If your duties for Microsoft involve selecting other Suppliers to work for Microsoft, make sure you do not have a conflict of interest. Carefully segregate your responsibilities to ensure you are acting in Microsoft's best interests.</td>
</tr>
<tr>
<td>▪ Read what the Code says about conflicts of interest.</td>
</tr>
</tbody>
</table>
Section: Protection of Assets, Confidential Information, and Intellectual Property

<table>
<thead>
<tr>
<th>Section Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of assets, confidential information, and intellectual property rights is vital for any company.</td>
</tr>
<tr>
<td>Microsoft’s business depends on respecting and protecting intellectual property such as copyrights, trade secrets, trademarks, patents, inventions, designs, and logos.</td>
</tr>
<tr>
<td>Microsoft also depends on keeping our users’ trust through keeping Microsoft systems and data secure and upholding strong privacy standards.</td>
</tr>
<tr>
<td>This section of the Code describes Supplier obligations in the following areas:</td>
</tr>
<tr>
<td>- Respecting and protecting the intellectual property rights of all parties;</td>
</tr>
<tr>
<td>- Protecting and using responsibly the physical and intellectual assets of Microsoft;</td>
</tr>
<tr>
<td>- Using Microsoft-provided information technology and systems only for authorized Microsoft business-related purposes;</td>
</tr>
<tr>
<td>- Complying with all Microsoft requirements and procedures for maintaining passwords, confidentiality, security, and privacy;</td>
</tr>
<tr>
<td>- Complying with the intellectual property ownership rights of Microsoft and others.</td>
</tr>
<tr>
<td>Let’s learn about how to comply with the Code’s requirements for confidentiality, data security, privacy, and physical security.</td>
</tr>
</tbody>
</table>
## Topic: Confidentiality

### Topic Introduction: Confidentiality

External Staff members often create, use, or come into contact with Microsoft’s intellectual property that is also Microsoft’s confidential information — in documents, meetings, telephone conversations, emails, and on Microsoft’s corporate network.

Suppliers sign a non-disclosure agreement agreeing to protect Microsoft confidential or proprietary information. This obligation applies both during and after the Supplier’s work with Microsoft.

### Scenario: “Information on the Network”

*In this scenario, an External Staff member, Kumar, is authorized to access the Microsoft corporate network. While saving a document to a team SharePoint site, Kumar discovers unsecured Microsoft confidential information about future product plans. He reports his discovery to his manager, Will.*

*Kumar, External Staff:* Will, I think you should see what I found on the Microsoft team site.

*Will, Supplier manager:* Sure. What’s up, Kumar?

*Kumar:* I stumbled on the launch plans. I wasn’t snooping—it was an accident. But you should see how much they’re planning to spend on the launch. Should I make a copy?
<table>
<thead>
<tr>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>How should the Supplier manager, Will, handle this situation?</td>
</tr>
<tr>
<td>Select the correct answer.</td>
</tr>
<tr>
<td>A. Tell Kumar to ignore the information and keep working.</td>
</tr>
<tr>
<td>B. Tell Kumar to copy the information because it might be useful.</td>
</tr>
<tr>
<td>C. Tell Kumar to not copy the information and notify his Microsoft contact about the unsecured information.</td>
</tr>
<tr>
<td>D. Tell Kumar to email the information to everyone on the project team so they know about the issue.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>The correct answer is C. External Staff members may occasionally see confidential information that has not been secured but should have been. Do not share the information with anyone else and do not use or transmit the information in any way.</td>
</tr>
</tbody>
</table>
### Question

Identify which of the following types of intellectual property could be considered Microsoft confidential:

*Select the correct response.*

- A. Source code, pre-release builds
- B. Product plans, technical specifications, and milestones
- C. Usability surveys, test results, or bug data
- D. All of the above

### Answer

The correct answer is D. All of these types of intellectual property may be confidential information.
Social Media Guidelines

Social media is a big part of many people’s lives, for both personal and professional reasons. Whenever you engage in social media, be sure to consider confidentiality concerns—especially when it comes to saying anything about Microsoft personnel, products, or plans.

Here are some basic do’s and don’ts:

- **DO** protect confidential information.
- **DO NOT** make announcements about projects or plans that are not your own.
- **DO** feel free to speak in support of major company announcements that have already been made public if you are inspired to.
- **DO** make your relationship to Microsoft clear when posting. Make it clear who your employer is and that they are a Microsoft supplier.
- **DO** recognize that anything you say can be viewed as an official company statement.
- **DO** be honest, accurate, and ethical at all times.
- **DO** understand the potential consequences of anything you post on social media.
# Key Learning Points

- Microsoft confidential information includes, but is not limited to, information relating to Microsoft’s technology and business that is not readily available or known to the general public.

- Sometimes confidential information is designated or marked “confidential” or “proprietary,” but not always.

- Confidential information can include sales and marketing information, and financial, legal or business data and strategies.

- External Staff members should protect Microsoft confidential information at all times. Use common sense and good judgment.

- Precautions that External Staff members should take to protect confidential information include:
  - Contact Microsoft immediately if Microsoft or third-party confidential information has been leaked.
  - Do not discuss information about Microsoft and its partners and customers in public places where third parties may overhear. This includes cafeterias and non-secure hallways and lobbies.
  - Do not share any Microsoft confidential information with friends, family members, or former colleagues or employees.
  - Discuss Microsoft confidential information with Microsoft employees only on a need-to-know basis.

- Depending on the security classification of the data involved, confidential data may need to be encrypted while in transit or where it is stored. Your Microsoft contact should work with a security professional to make that determination.

- Read what the [Code](#) says about confidentiality.
Topic: Protecting Data, Part 1: Data Security

**Topic Introduction: Protecting Data**

Data is essential to business innovations at Microsoft. Data-driven, actionable intelligence is an essential part of how we help our customers be productive and achieve more. With the increased data capture and analysis required to deliver these capabilities, it's imperative that we maintain our strong security and privacy practices, so that customers know their data is safe.

Protecting data has two components—Data Security and Privacy—which we'll cover over two sections of this course.

**Data Security** is about protecting data from things like loss, misuse, unauthorized access, or disclosure. In this section, we'll look at how you can protect data by preventing security breaches.

**Privacy** is about using data responsibly, which starts with ensuring users know what data we collect and how we use it. It also means giving them options that put them in control of their data. In the Privacy section, we'll look at your responsibilities in supporting Microsoft's commitment to privacy.

When Microsoft protects data through strong security and respectful privacy practices, we build customers' trust. When customers trust Microsoft with their data, we're able to provide them with our most innovative, data-driven products and services.

**Topic Introduction: Data Security**

To protect data, it's important to be aware of common ways data security may be breached.

You're probably already familiar with phishing and malware, but you might not be aware of how sophisticated the attacks can be — or what steps you can take to avoid being a victim. We'll take a look at those in this section.

**Phishing** is an attempt to acquire your information, such as your Microsoft credentials, by masquerading as a legitimate offer or a legitimate request for action or information. Phishing attempts may have the goal of defrauding you of money, obtaining sensitive information for competitive advantage, or installing malware on
Malware is malicious software used to disrupt computer operation, gather sensitive information, or gain access to computer systems. Malware may be installed when you open an email attachment, visit a malicious site, or install untrustworthy software.

Activity: Recognizing Phishing

Is the email shown here suspicious?

From: Microsoft Support Team
<support@microsoft.com>
Sent: Wed 6/3/2016 8:30 AM
To: Erin Oliver
Subject: Account Suspended

Good Afternoon!

Our system detected some unusual activity with your account. We've temporarily suspended your account — please log in at the link below to verify your account details and reactivate. If you fail to do so within 4 hours, we will permanently disable your account.

http://login.microsoft.com

Thanks,

Microsoft Support Team
(800) 642-7676
support@microsoft.com

© 2016 Microsoft. All rights reserved.

Here are tips about how to recognize phishing emails.
Branding and Contact Information that Appear Legitimate
Phishing emails often contain a mix of real and false information.

Remember that the presence of a company’s logo or copyright notice does not necessarily mean the email is legitimate.

Similarly, the presence of a phone number and email address—even ones that you know are correct—does not mean the rest of the email is legitimate.

Details Not Quite Right
Phishing emails often contain details that may not seem quite right.

This is a somewhat strange greeting. Why does it say afternoon specifically? Why have an exclamation point? Would a legitimate email perhaps put your name in the greeting?

A Reason for Action
Phishing emails often give you some reason to take action—though of course many legitimate emails do the same.

This sentence could be the start of a legitimate email, but it could also be an invented situation designed to get you to click on something.

Misspellings and Errors
Phishing emails often contain spelling or grammar issues.

This email has errors. Legitimate Microsoft emails are typically reviewed for spelling and grammar prior to being sent.

Threats
Phishing emails often contain threats.

They try to convince you that you must do what they are asking, or face negative consequences.

Hidden URLs
Phishing emails often contain hidden URLs.

In an actual email, if you have any reason at all to be suspicious, think twice before clicking any link.

Hover over links before clicking them. Does the hidden URL go to the domain name you were expecting? If not, you are probably being directed to a malicious site.
If you are on a touch-enabled device and cannot hover over a link to see where it goes, do not click any link unless you are certain the email is from a trusted source.

Scenario: “Expired Software”

In this scenario, an External Staff member named Amber is using a software program to help with a Microsoft deliverable, but today she gets an error message that says the license has expired, and she cannot launch the software.

Amber, External Staff: My license is expired?? That’s impossible! I’m sure we renewed that. All I know is I need to finish this deliverable today. I bet I can find a key generator online to help me unlock the software for now, and then we can sort out our licensing later.

Question

Is it OK for Amber to use the downloaded software to generate a pirated key to unlock the software?

Select the correct answer.

A. Assuming her anti-malware software is up to date and running, she should be OK to run the software.

B. She can download the software, but she should remove it immediately if her system becomes unstable.

C. Amber should not download a key generator under any circumstances.
## Answer

The correct answer is C. Amber is illegally obtaining access to third party software. Not only is this against the law and Microsoft policy, but cybercriminals use free or pirated software as a way to download malware onto the victim's computer. Once installed, malware is hard to remove.

## Key Learning Points

- **Carefully examine all emails:**
  - Carefully review email attachments, instant messages, and social media links before clicking to open them. Even if they appear to be from a trusted sender, watch out for any indicators of phishing.
  - Look for any unexpected URLs in links or other details that do not seem quite right.

- **Pay special attention if asked to enter credentials on a website.**

- **Develop good password habits:**
  - Use strong passwords that contain a mix of letters, numbers, and special characters.
  - Use different passwords for different sites. Never re-use your Microsoft password on other sites or services.
  - Store passwords according to MSIT Approved Policy.

- **Enable secure login and multi-factor authentication when available.**

- **Keep your devices safe from malware:**
  - Install Microsoft and third party software updates when prompted.
  - Do not download unknown software or run programs that you do not recognize. Under no circumstance should you download or use pirated software.
Topic: Protecting Data, Part 2: Privacy

Topic Introduction: Privacy

Security is necessary to protect data, but it is not enough on its own; we also must think about our customers’ privacy.

We treat our customers’ personal data as you would treat your own: carefully, responsibly, and discreetly.

You can help us maintain trust by ensuring that you follow the Microsoft Corporate Privacy Policy in all the work you do for us.

Suppliers must support Microsoft privacy principles:

- When designing products and services
- In marketing campaigns and all customer communications
- When collecting and handling personal data
- In the process of maintaining or disposing of personal data

Scenario: “Subcontracting a Website”

In this scenario, a Supplier marketing firm is creating a campaign for Microsoft for the release of a new Windows 10 app developer toolkit. The campaign includes creating a new developer website, which the marketing firm is subcontracting to another company. Helena, one of the marketing firm’s employees, asks her coworker Veena about some concerns she has.

Helena, External Staff: Since we’re subcontracting this website, are we responsible for our subcontractor following Microsoft’s privacy standards?

Veena, External Staff: We aren’t collecting any sensitive information are we? I mean, it’s a developer site, so the data doesn’t seem very personal.

Helena, External Staff: I’m sure we want site visitors to opt-in to the campaign’s email list. And if people want to participate in the discussion boards, they’ll need to create a profile.
Veena, External Staff: OK, true—the site will collect some data. But I think managing it is the subcontractor’s responsibility.

<table>
<thead>
<tr>
<th>Question 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Helena and Veena’s marketing firm responsible for the subcontracted website meeting Microsoft’s privacy standards?</td>
</tr>
<tr>
<td>Select the best answer.</td>
</tr>
<tr>
<td>A. Yes. If the website is collecting any data at all, Helena and Veena’s firm must ensure that the subcontractor meets Microsoft’s privacy requirements.</td>
</tr>
<tr>
<td>B. It depends. As long as the website doesn’t collect any of users’ personally identifiable information, there is no data privacy concern.</td>
</tr>
<tr>
<td>C. No. Because they are subcontracting the work, any privacy obligations reside with the subcontractor.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Answer 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>The best answer is A.</td>
</tr>
<tr>
<td>Microsoft Suppliers should ensure they—and their subcontractors—meet all the same privacy standards and legal obligations that Microsoft is committed to.</td>
</tr>
<tr>
<td>Microsoft is committed to handling all customer data respectfully. Any time a website collects customer data, users must be provided notice and consent mechanisms and appropriate privacy controls.</td>
</tr>
</tbody>
</table>
### Question 2

How should Helena and Veena ensure the website privacy considerations are addressed appropriately?

*Select all that apply.*

A. Review Microsoft’s privacy policies with the subcontractor and get their written agreement that they will adhere to them.

B. Hire a third party privacy consultant to assess the situation and follow their recommendations.

C. Ask their Microsoft contact if he or she has engaged Microsoft’s Privacy experts to review the project.

### Answer 2

The correct answers are A and C.

Helena and Veena’s marketing firm should review the Microsoft [Supplier Data Protection Requirements](#) with their subcontractor.

Any and all of the privacy impacts of the project with Microsoft should be reviewed by one of Microsoft’s privacy experts before work begins.

Helena and Veena should ask their Microsoft contact about it and ensure that a privacy review is planned.

Microsoft’s privacy experts should be engaged to:

- Determine what privacy rules apply to the project’s data use
- Help the team determine the best way to notify users about what data is collected and why
- Where appropriate, provide people with choices and controls over what data is collected.
Microsoft’s Privacy Experts

From a privacy perspective, all projects should start by asking and answering the following three questions, which Microsoft’s privacy experts can help with:

1. What data is required for this project and why?
2. What rules apply for the appropriate use and management of the data?
3. How can we help the user understand why the data is needed and show them what they get in return for their data?

Microsoft’s privacy experts can also identify any data handling requirements that apply to your project—for instance, you may be required to encrypt, de-identify, or track certain data, and to enforce data retention policies. Smart data handling can help prevent a security breach impacting privacy.

Whenever a project involves handling or accessing customer, employee, or partner information, plan ahead and have your Microsoft contact work with the privacy experts on his or her team to surface requirements and meet them.

If you ever have questions about privacy impacts as you do your work, your Microsoft contact can engage these experts at any time.

Question 3

What about when a privacy incident arises? Do you know which of the following are privacy incidents that should be reported to Microsoft?

Select all that apply.

A. Personal data is accidentally retained longer than the specified retention period.

B. Someone posts a list of Outlook.com email addresses on a website along with corresponding passwords.
C. An app or website is missing a link to a privacy statement.

D. An unencrypted mobile device is lost. Theft is not suspected.

E. A password-protected laptop containing unencrypted personal data is stolen.

F. A promotional email is lacking the approved email footer that links to an opt-out mechanism.

G. Data is processed in a way not authorized by an Enterprise Customer.

**Answer 3**

All of these are examples of privacy incidents that should be reported.

If personal data is lost, stolen, or at any point may have been inadequately protected or inappropriately accessed, this should always be reported. As you can see, there are other, subtler forms of privacy incidents too.

It is important that you can spot a privacy incident, and that you report any incidents promptly!

You can report a privacy concern the same way you report any Supplier Code of Conduct concern.
<table>
<thead>
<tr>
<th>Key Learning Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ You are contractually obligated to meet the same privacy standards and legal obligations that Microsoft itself has, and you must enforce privacy compliance with anyone whom you subcontract.</td>
</tr>
<tr>
<td>▪ Privacy requires giving choices and controls over data collection and following smart data-handling practices to prevent security breaches.</td>
</tr>
<tr>
<td>▪ Data collection must always design in:</td>
</tr>
<tr>
<td>- An appropriate notice and consent experience prior to collection.</td>
</tr>
<tr>
<td>- An explanation of why the data is being collected and what it will be used for.</td>
</tr>
<tr>
<td>- A link to the appropriate Microsoft privacy statement, or for offline data collection, a short privacy statement on the data collection form.</td>
</tr>
<tr>
<td>- Clear indication of which fields are required. Fields should only be required if necessary to provide the service that the customer is signing up for.</td>
</tr>
<tr>
<td>- Permission and contact preference questions, if the data may be used for marketing activities.</td>
</tr>
<tr>
<td>▪ Your Microsoft sponsor/contact can connect you with a privacy expert at the company to help ensure that privacy controls are designed into your collection experience.</td>
</tr>
<tr>
<td>▪ Report any privacy incidents promptly in the same way you report any Supplier Code of Conduct concern.</td>
</tr>
<tr>
<td>▪ Where your company handles Microsoft personal data outside the Microsoft environment it must follow the Microsoft Supplier Data Protection Requirements. Make sure you have read these requirements to support your company’s compliance to the standards.</td>
</tr>
<tr>
<td>▪ Read what the Code says about data security and privacy.</td>
</tr>
</tbody>
</table>
## Topic Introduction: Physical Security

Physical security is the protection of everyone and everything in your work environment from physical harm, loss, or disruption—for instance, securing buildings from unauthorized access, securing property from theft, and providing protection in situations such as fire or natural disaster.

In addition to the confidentiality and data security practices we already covered, maintaining physical security is also essential for protecting Microsoft from unauthorized access to information and data.

## Scenario: “New Project”

*In this scenario, an External Staff member named Carlos has just started a new project where he will work on a Microsoft campus for a two-month period.*

*Carlos, External Staff:* I haven’t worked on site at Microsoft previously, so I have a few questions. First of all, I know I need to use my badge to get into the building. How about the rest of the time—can I just keep it in my wallet? That seems like the best way to keep it safe.
**Question 1**

Is it OK for Carlos to keep his badge in his wallet while he is working at Microsoft?

*Select the best advice.*

- **A.** The most important thing is to wear the badge visibly at all times while on site. It is not acceptable to keep it in his wallet because it would not be visible.
- **B.** The most important thing is to prevent unauthorized access to his badge. Keeping it in his wallet could be a good option or keeping it in his locked desk.
- **C.** The most important thing is to keep the badge with him at all times while on site. Keeping it in his wallet is acceptable so long as he always carries his wallet.

**Answer 1**

The best answer is A.

Your badge should always be visible while working at Microsoft. Carlos should wear it on a lanyard around his neck or on a zip reel on his hip.

This allows Security and other personnel to more easily notice whether the people they see on campus are appropriately badged.

**Scenario: “Lunch Date”**

*Carlos’ wife Joni is going to be in the area at lunch time, and they decide to have lunch together at Microsoft.*

*Joni, visitor:* So, I'll be there a little before noon. Where should I meet you?

*Carlos, External Staff:* Let’s meet near the entrance to the café. When you park in the
lot, it will be the building on the south side.

Joni, visitor: Oh—can I go directly there, or do I need to check in first or something?

Question 2

What should Carlos tell Joni?

Select the best advice.

A. I’ll have my badge, so you’ll be fine with me. If you can’t get in the door by the cafe, just text me and I’ll come let you in.

B. Yes, you will need to check in at reception first. After you get your visitor pass, you can meet me at the café. Reception can point you in the right direction.

C. Ah—that’s right. Check in at reception first, and I’ll meet you there in the lobby.

Answer 2

The best answer is C.

Visitors must check in, get a visitor pass, and be escorted at all times.

To maintain strong physical security at Microsoft, all people on campus for any reason should have a badge or visitor pass visible at all times.

Carlos should plan to meet his wife in the lobby. After she gets her visitor pass, they can walk to the café together.
Question 3

After lunch, Carlos walks out to the parking lot with Joni. When he returns to enter the building, he scans his badge at a side door. As he opens the door, another person approaches and grabs the door before it closes. What should Carlos do?

Select all options that are good advice.

A. If they appear to be wearing a badge, no action is needed.
B. If they do not appear to be wearing a badge, tell them they cannot come in.
C. Ask the person to scan their access card before entering.
D. If the person does not have an access card or has one that does not work, direct them to reception.

Answer 3

The correct answers are C and D.

To maintain strong physical security at Microsoft, it’s important for everyone to scan their access card at controlled doors.

While everyone is required to have a visible badge, just seeing a badge at a glance isn’t sufficient for controlling access.

People who are legitimately on campus should never hesitate to scan their access card and should not be offended by being asked to. It’s part of what we do together to maintain a secure environment.

If the person does not have an access card or has one that does not seem to grant access to the door, direct them to reception for assistance.
## Key Learning Points

- Physical security measures help keep people and property secure at Microsoft—which also helps us keep our data secure and make sure confidential information stays confidential.
- Controlling access to our facilities is our first line of defense.
- Wear your badge or visitor pass visibly at all times.
- Always escort your guests.
- Never allow anyone into our buildings unless they have authorized permission.
- Read what the [Code](#) says about security.
Reporting

If you wish to report questionable behavior or a possible violation of the Supplier Code of Conduct, please contact Microsoft through any of the following methods:

**Call:**
In the U.S.: 1-877-320-MSFT (6738)
Outside the U.S. (collect): 1-470-219-7087

**Email:** Business Conduct and Compliance alias (buscond@microsoft.com)

**Online:** www.microsoftintegrity.com

**Mail:**
Microsoft Corporation
Corporate, External, and Legal Affairs (CELA) Group
One Microsoft Way
Redmond, WA 98052

**Fax:** 1-425-708-7177

Microsoft will maintain confidentiality to the extent possible and will not tolerate any retribution or retaliation taken against any individual who has, in good faith, sought out advice or reported questionable behavior or a possible violation of this Supplier Code of Conduct.

**Congratulations on completing this course!**

Additional Resources

- Microsoft’s Supplier Code of Conduct
- Microsoft’s Anti-Corruption Policy for Representatives
- Supplier Security and Privacy Assurance Program