HSBC
Remote Working

Table of Contents

Introduction

Page 1
Description: The header contains the course title, company logo and the close button. The footer contains the navigational buttons as well as the page numbers. This is the same throughout the course.

Screen text: SECURING INFORMATION, PROTECTING REPUTATION

Page 2
Description: Image of a woman using a laptop is to the left, text is to the right.

Screen text: Welcome

Some members of staff need to access HSBC's systems outside of their office or branch (for example, at home). This is known within the Bank as remote working. This course will help you understand and manage the information security risks associated with remote working.
You will learn:

- Why it is important to keep information secure
- What are the key information security risks when you are remote working
- The practical steps that you can take to keep information secure
- How you report an information security incident
- Where you can obtain further help and guidance

Page 3

Description: An image of a woman using a laptop is to the left. Text is to the right.

Screen text: About the course

Use the Next and Back buttons to go forwards or backwards through the course.

On some pages, you will not be able to move forwards until you have completed all of the interactions on the page.

The course will take approximately 15 minutes to complete. You do not need to do it in one session. You can leave at any time – when you return, you will have the option to rejoin where you left off.

You can also use the Menu button at any time to access pages that you have already visited. CLICK ON the Button opposite for more information on how to use the Menu.

At the end of the course, you will take an assessment. You must score 80% or more to complete the course.

How to use the Menu

The Menu button allows you to navigate to any screen in the course you have previously visited.
► expands a chapter heading to reveal links to all pages in that chapter
▼ minimises an open list of pages to show just the chapter heading

Click on the title of any page labelled Unlocked to move to that page in the course.

You cannot move to any page labelled Locked.

Click on the red icon to close the Menu and return to the course.

CLOSE pop-up

Page 4

Description: An image of a man and a woman each using a mobile device is to the left. Text is to the right.

Screen text: Important

Employees are only allowed to remote work if controls are in place to enable them to work securely.

Before you are allowed to remote work, your line manager must check that you have completed this training and that you have passed the end of course assessment. You will also need to complete the Health and Safety elearning course (which is listed in the HSBC Business School).

CLICK ON the Next button to continue.

Page 5

Description: Image of staff at a meeting.

Screen text: Why is this important?

Our day-to-day business relies on the information that we hold about:

- Our organisation
- Our customers
- Our employees
- Our suppliers

Everyone in our organisation has a duty to keep this information secure in accordance with HSBC's policies and standards. This helps to protect our reputation and avoid sanctions from our regulators.

CLICK ON the Next button to continue.

Page 6

Description: An image of a man using a BlackBerry is to the left, text is to the right. Three buttons are to the far right.

Screen text: What are the risks?

When you are remote working, information is not protected by the controls that exist within HSBC premises. In addition, you may have less control over your surrounding environment (for example, in public places). This creates a broad range of potential risks, including:

- Information may be lost, inadvertently disclosed or stolen
- Wireless or other computer networks may not be secure (allowing information to be intercepted)
- Telephone conversations may be overheard

To manage the specific risks associated with remote working, you must take extra care to ensure that information is protected.

CLICK ON the Buttons opposite to learn more.

Lost Wireless Devices

According to a 2012 report from Credant Technologies, 8,016 lost mobile devices were found at seven major airports. 43% of these were laptops, 45% were smartphones and tablets and 12% were USB drives. Just 52% of the devices were returned to their owners.
Also in 2012, Symantec conducted a study in which researchers intentionally lost 50 smartphones in five different cities to see whether the finders attempted to access information.

Around 89% of the finders viewed personal information and 83% tried to access business-related information stored on the devices.

Lost and Stolen Documents

Over the past few years, there have been a number of high profile security breaches associated with lost documents. For example:

- In New Zealand, a major Healthcare provider was forced to apologise after patient records were found in the street. An investigation revealed that they had been stolen from an employee's car

- In 2012, the London Metropolitan Police was criticised after a commuter found secret documents on a train. The documents, which outlined security measures for the 2012 Olympics, had been lost by a senior officer

But this doesn't just happen to other people – similar breaches have occurred at HSBC. Your vigilance is essential to stop this happening.

The Billion Dollar Laptop Study

In 2012, security experts estimated that the average cost of a lost laptop is nearly 50,000 USD. 80% of this cost is attributable to remedying the information breach that could result from the loss.

The study states that financial services firms are amongst those that would suffer the greatest damage from a lost laptop.

For example, a few years ago, the Nationwide Building Society (a UK financial services institution) lost 11 million customer records when a laptop was stolen from an employee's home. Nationwide was criticised for allowing the information to be stored on the laptop and delays in starting the investigation. As a result, it was fined almost 1 million GBP by the financial services regulator and suffered massive damage to its reputation.

CLICK ON the Next button to continue.

Page 7

Description: An image of a smiling woman is the left. Text is to the right.

Screen text: Securing information, protecting reputation

As the examples illustrate, information security breaches could be very damaging to our business. They also have the potential to undermine our core values which require everyone in our organisation to be:

- Dependable and do the right thing
- Open to different ideas and cultures
- Connected to customers, communities, regulators and each other

The next section explores our Remote Working Policy and highlights the key risks when you are preparing to remote work, travelling and working from home. At each stage it also explains the practical steps that you should take to manage the risks.

CLICK ON the Next button to continue.

Preparing to Work Remotely

Page 8

Description: An image of a woman examining a file is to the left, text is to the right, five buttons are to the far right.

Screen text: Information classification

Whenever you are handling information (whether inside or outside the office) you must consider its classification and value to the organisation.

All information must be classified into one of the four categories shown opposite. This determines how the information should be handled, including its distribution, storage and disposal.

For further details, please review the Information Classification Policy or the Information Classification Illustrative Examples.

CLICK ON the Buttons opposite for a reminder of the classifications.

Highly Restricted

Poses a massive risk.
This information is only available to a very limited audience who are authorised to see it. Examples include: merger/acquisition plans and passwords/logon codes that grant access to HSBC's systems and electronic files.

Restricted

Poses a moderate to major risk.
This information is generally only available to those who need to know. Examples include: personal information about customers, shareholders, employees, operational budgets and strategic plans.

Internal

Poses a minor risk.
This information is available to all employees, but is proprietary to HSBC. Examples include: HSBC policies, organisational charts and employee at-work contact information.

Public

Poses an insignificant risk.
This information is available to external parties and includes information that has been intentionally disclosed by HSBC. Examples include: published press releases and marketing materials on display at branches.

Public information does not require any special handling or protection.

Non-HSBC

Information that has originated from outside HSBC.
This is information that has been generated by companies external to HSBC.

CLICK ON the Next button to continue.

Page 9

Description: An image of a woman reading is on the left, text is on the right.

Screen text: Before you leave the office

You should start to manage the information security risks associated with remote working long before you leave the office.

Always think very carefully about how to prepare for remote working:

- What will you be working on?
- What tasks do you need to complete?
- What information do you need to complete these tasks?
- What is the most secure way to access this information?

CLICK ON the Next button to find out what you should do.

Page 10

Description: There is of a hand on a mouse on the left, text and buttons are to the right.

Screen text: Scenario

It's almost the end of the day and Tim is preparing to work from home tomorrow on an important report that is due at the end of the week.

Tim will need to access several documents that have been classified as Restricted.

How should Tim access these documents when working from home?

CLICK ON one of the Buttons opposite to indicate the most secure way to access the information.

1. Print the documents he needs as it is safer to review them this way. (Incorrect)

2. Use his remote access to view the documents on HSBC's systems. (Correct)

3. Send the documents to his personal email address. (Incorrect)

Tim should use his remote access to view the documents on HSBC's systems.

Options 1 and 3 are not secure for the reasons outlined below:

- Printed documents should only be taken out of the office where absolutely necessary to reduce the risk of loss or unauthorised disclosure

- Working at home is NEVER a valid reason for sending Bank information to your personal email address. Personal email accounts are not secure, so it could result in the information being lost or stolen. Sending Bank information to your personal email address is a serious breach of our policy and could result in disciplinary action being brought against you (up to and including dismissal)

CLICK ON the Next button to learn more about information classification and the steps you should take to protect information.

Page 11

Description: The image on the left shows a laptop and a scientific calculator, text on the right

Screen text: Handling information outside the office

The only information that is absolutely safe to handle outside HSBC's secure systems is Public information. All other classifications should be treated as follows:

Documents
Printed documents should only be taken outside the office if absolutely necessary.

- Only take what you need
- Make sure you know what you are taking off site
- Dispose of documents securely (e.g. return them to the office for secure disposal)

Electronic
Always use your secure remote access ID to access information on HSBC's systems.

- Only download information onto an HSBC laptop if absolutely necessary (transfer it back to HSBC's systems at the earliest opportunity and delete it from the hard drive)
- Never forward any HSBC information to your personal email address

CLICK ON the Next button to continue.

Travelling

Page 12
Description: There is an image of a train on the left and text on the right.

Screen text: Travelling

When you are travelling on public transport, you should consider the information security risks:

- Is it an appropriate place to work?
- Can your computer or documents be seen by others?
- Can your conversation be overheard?
- Is your bag or case secure?

CLICK ON the Next button for more information on how to manage these risks.

Page 13
Description: There is an image of a woman using a mobile phone on the left and text on the right.

Screen text: Scenario

Hi-Leng is on her way home in a very busy train carriage. She receives a call on her work mobile phone from one of her colleagues, Ben.

He has a meeting first thing tomorrow and needs some information urgently from Hi-Leng to help him prepare.

What should Hi-Leng do?

CLICK ON one of the Buttons opposite to indicate the most secure option.

1. Discuss with Ben what he needs and provide the information over the phone. (Incorrect)

2. Offer to call Ben back when she gets home. (Correct)

3. Ask Ben what he needs, make notes and then look at her laptop to see if she has the information. (Incorrect)

Hi-Leng should offer to call Ben back when she gets home.

Options 1 and 3 are not secure for the reasons set out below:

On a busy train, a telephone conversation is likely to be overheard. There is no knowing who is listening or what they might do with the information

She should also take care when making notes or accessing information on her laptop – other people in the carriage may be able to see the screen

CLICK ON the Next button for more advice on how to protect information whilst travelling.

Page 14

Description: The image on the left shows two employees talking.

Screen text: Keeping information secure whilst travelling

The use of mobile devices such as BlackBerrys and laptops has become an essential part of working at HSBC.

However, you must protect the information you hold from inadvertent disclosure.

- Exercise caution in public areas when viewing HSBC information and ensure that it cannot be read by anyone else
- If you use your laptop in public areas, use a screen protector
- Shut down your laptop when travelling (and lock mobile phones)
- Make sure documents are transported securely
- Hold business conversations in private. If you are in public, offer to return the call once you are in a private location such as at home or in a hotel room

CLICK ON the Next button to continue.

Working at home

Page 15

Description: The image on the left shows a laptop on a domestic table, which the screen displaying the HSBC intranet

Screen text: Working at home

Information security doesn't stop when you get home. When remote working, you should consider:

- What information do you need to have at home?
- Is information kept secure from those who are not authorised to see it (for example, people you live with)?
- Are electronic devices stored securely when not in use?

CLICK ON the Next button to learn about protecting information at home.

Page 16

Description: There is an image of a woman using a laptop in a domestic environment to the left. Text is in the centre with three buttons on the right.

Screen text: Scenario

Natalia has been working from home, completing her team's appraisals. She has been working on her HSBC laptop, but has also referred to written notes that she made during meetings with the team.

It's the end of the day and she is planning to go out for dinner. There is no-one else in the house, but her partner is due home soon. How should she protect the information?

CLICK ON one of the Buttons opposite to indicate the most secure option.

1. Close the computer lid and put the documents on top. (Incorrect)

2. Take the computer and the documents with her. (Incorrect)

3. Shut down the laptop and store it (and the documents) securely. (Correct)

Incorrect

When leaving a computer for an extended period of time, it should be shut down and stored in a secure place, out of view. As the documents contain employee personal information, they are likely to be classified as Restricted. Therefore, these need to be stored securely (for example, in a locked drawer).

Options 1 and 2 are not secure for the reasons set out below:

- It is not sufficient to simply close the computer lid and place the documents on top. This does not stop other people in the house looking at the documents. It also does not provide adequate security for the laptop or documents in the event of a burglary

- She should not take them with her when she goes out – this would create an unnecessary risk of loss or theft

CLICK ON the Next button for some advice on keeping information secure when working at home.

Page 17

Description: There is an image of a red mug on the left, there is text on the left.

Screen text: Keeping information secure at home

You must keep information secure when working at home to prevent unauthorised access and reduce the risk of it being stolen.

- Make sure your working environment is secure (for example, your screen is not overlooked)
- Lock mobile devices if they are left unattended for a short period and shut them down if they are unattended for an extended period (generally over three hours) or overnight
- Store mobile devices securely when not in use (for example, in a locked cabinet or tethered with a cable)
- Exercise caution when taking Internal, Restricted or Highly Restricted physical information away from HSBC premises:
    - Consider carefully whether you need to take documents outside the office and take the minimum information required
    - Store documents securely (e.g. in a locked drawer or, if necessary, a lock box)
    - Dispose of documents securely (e.g. return them to the office for secure disposal)

CLICK ON the Next button to continue.

Reporting Breaches and More Information

Page 18

Description: An image of a man using a mobile phone is on the left, there is text in the centre and buttons on the right.

Screen text: Information security breaches

If you know or suspect that a security incident has occurred, it is your responsibility to report it immediately.

Remember - you are entirely responsible and accountable for protecting information entrusted to you and you must exercise a duty of care and attention.

Do not delay in making a report - the sooner a report is made, the sooner action can be taken to identify and manage the risks. As the cases highlighted earlier in the training illustrated, delays can also result in fines and other enforcement action by regulators.

CLICK ON the Buttons opposite for examples of potential incidents and what action you must take to report them.

Examples

Examples of security incidents include:

- Loss or theft of an HSBC issued computer, mobile device, or portable media (e.g. USB, CD)
- Human or equipment error resulting in loss of Internal, Restricted or Highly Restricted information (e.g. documents are lost)
- Possible unauthorised access to Internal, Restricted or Highly Restricted information (e.g. it is left unattended in a public place)

If you suspect something is wrong (even if you are not sure) report it immediately.

How to report
You must report any incident to line management and the Incident Management Team as soon as possible.

The Incident Management Team will investigate the incident and take steps to minimise the impact on HSBC and others who may be affected (for example, customers and employees). They will also consider any underlying issues to try to prevent the incident happening again.

To ensure that incidents are reported quickly when you are remote working, it is very important that you familiarise yourself with the correct procedure. In particular, make sure you know what to do and where to find relevant contact information should an incident occur. Speak to your Business Information Risk Officer (BIRO) for further information (including contact details for your Information Security Risk team).

CLICK ON the Next button to continue.

Page 19

Description: The image on the left shows a keyboard with a key showing the HSBC logo. Text is on the right.

Screen text: More information

This course has explored your responsibilities when you are remote working.

More information (including links to policies and standards and how you can contact your Business Information Risk Officer) can be found on the Information Security Risk Intranet.

You must now take the end of course assessment. Your line manager will need to check that you have completed the course and passed the assessment before authorising your remote working secure access.

CLICK ON the Next button for instructions on how to complete the end of course assessment.

Page 20

Description: The image on the left shows a hand picking up a brick from a brick wall. Text is on the right.

Screen text: The course assessment

You have now completed the learning section of this course. If you wish, you can use the Menu function to revisit any of the pages before starting the assessment (note: the Menu will not be available during the assessment).

The assessment contains 5 questions. For each question, select an answer and then CLICK ON the Submit button. This will automatically move you to the next question.

At the end of the assessment, you will see the score you achieved. A separate pop-up window will also show you the questions you answered incorrectly and guide you to sections in the course where you can revise your knowledge using the Menu.

You must score 80% or more to complete the course.

If you are ready to take the assessment, CLICK ON the Next button to begin.

Assessment

Question 1

Sam is preparing to work on a report classified as Restricted when she is working remotely tomorrow. Which of these is the best way to access the information she will need?

A. Copy the information onto the hard drive of a laptop computer
B. Send the report to her personal email account so she can work on her home computer
C. Take paper copies of everything she will need
D. Use her remote access to view the information on HSBC's systems

Question 2

What security precautions are required when taking physical documents out of the office? (select all that apply)

A. Take the minimum amount of information out of the office
B. Send an email to your line manager listing what you are taking
C. Transport the documents securely
D. Make sure that the documents are disposed of securely when no longer required

Question 3

Which of the following is required before an employee is allowed to work remotely? (select all that apply)

A. They must complete the Remote Working elearning course and pass the assessment
B. They must obtain line manager approval for remote working
C. Their home computer equipment must be checked by IT
D. They must complete the Health and Safety elearning course

Question 4

You are visiting a client and will be staying overnight in a nearby hotel. Before going out for dinner, you decide to take your luggage into the hotel from your car. What should you do with your laptop computer to keep it secure?

A. Make sure it is switched off and leave it on the back seat of your locked car
B. Make sure it is switched off and store it securely (for example, in the hotel/room safe, if one is available)
C. You should screen lock it and leave on the desk in your hotel room
D. You should take it with you when you go out for dinner and leave it in the cloakroom at the restaurant

Question 5

You and a colleague are early for a meeting at a customer's office. Your colleague suggests that you run through the presentation and discuss your strategy at a local coffee shop. When you arrive, the coffee shop is quite crowded. What should you do?

A. It's okay to have a detailed discussion about the customer's account and review documentation
B. You can have a detailed discussion about the account, but should not review documentation as there is a risk that it may be left in the coffee shop
C. It's okay to have a general discussion, but you should not discuss or review detailed customer information
D. You should leave the coffee shop and go to the customer's office. It would then be okay to have a detailed discussion in the customer's reception area

Question 6

Liz is on a busy train when a member of her team calls to discuss a customer complaint. What should Liz do?

A. Have an open conversation to understand the complaint and give her colleague advice on how to resolve it
B. Ask her colleague to explain the complaint and start making notes so that she can deal with the matter properly later on
C. Say she will call her colleague as soon as she gets to her destination as she is on a train and can't speak due to confidentiality
D. Tell the colleague to email details of the complaint to her personal email address so she can review it when she gets home

Question 7

Which of these precautions should you take when you are travelling with HSBC mobile devices, such as a laptop, or paper documents? (select all that apply)

A. Shut down your laptop when travelling
B. Work on messages or documents only where you are confident you cannot be overlooked
C. Put a sticker or label on mobile devices that identifies it as belonging to HSBC
D. Consider a screen protector for your laptop if you work on the train

Question 8

Xao has been working at home on some Restricted documents and no longer needs the drafts he has printed. What should he do with these copies?

A. Keep them in a file at home
B. Rip them up and put them in the general waste
C. Put them in the recycling bin for paper collection
D. Return them to the office for secure disposal

Question 9

Which of the following HSBC documents are okay to review in a crowded public place?

A. A marketing brochure classified as Public
B. A telephone list classified as Internal
C. A customer complaint classified as Restricted
D. A merger proposal classified as Highly Restricted

Question 10

Sam is working from home. Which of the following would be a breach of information security?

A. He leaves his computer unattended for 30 minutes with the screen locked
B. His screen can be seen by members of the public walking along the pavement outside
C. He accesses documents classified as Restricted using his secure remote access
D. He does not lock documents classified as Public in a drawer when he leaves his desk

C. You should look for it at home that evening and, if you cannot find it, report the loss the following day
D. You should telephone the train company to report it as lost. If they are unable to locate it after a week, report it to your line manager