|  |  |
| --- | --- |
| Assessment Title | Workplace Cybersecurity Process |

## Competency Details

|  |  |
| --- | --- |
| Unit code/s and title/s | BSBXCS402 Promote workplace cyber security awareness and best practices |
| Qualification code/s and title/s | ICT50220 Diploma of Information Technology |
| Business unit/Work group | Business and Arts/IT Studies |

## Instructions

|  |  |
| --- | --- |
| Method/s of assessment | Questioning (Written)  Questioning (Oral)  Observation (Presentation) |
| Overview of assessment | This assessment will require you to complete written and oral answers for questions on the tasks listed below.  You will also complete practical tasks, create a presentation and take screenshots of their evidence of completion |
| Task/s to be assessed | In this assessment the student will be researching aspects of the following topics:   * Identify cybersecurity threats and trends * Review and update the company policy / procedures * Promoting workplace cyber security * Manager catchup |
| Time allowed | Refer to your schedule for submission dates |
| Location of assessment | Assessment can be completed anywhere with access to the resources required. (see Resources Required section below) |
| Decision making rules | To receive a satisfactory outcome for this assessment you must complete all parts correctly.  Word counts are provided as guidance only. |
| Assessment conditions | This assessment must be undertaken where the conditions replicate noise levels and interruptions that people typically experience working in the ICT industry.  This is unsupervised assessment and you may access any required resources.  Task 3: Promoting workplace cyber security Question 6 is a group task the remainder of the assessment work must be completed as an individual. |
| Resources required | Class computers will need to be provided with:   * Word processing software such as Microsoft Word. * Presentation software such as Microsoft PowerPoint * Communication/Recording software such as Microsoft Teams   You will need to have access to the various ITWorks Organisational Policy and Procedures located on Learn in the Assessment Documents and Submission Links topic (refer to the Assessment Support Documents for Students - ASDS).   * ITWorks-generic-security-policy.docx * ITWorks-security-policy.docx * ITWorks-Information-Classification-and-Handling-policy.docx * ITWorks-confidentiality-policy.docx * ITWorks-data-protection-policy.docx * ITWorks-backup-procedure-policy-procedure.docx * ITWorks-Log-ICT-Service-Requests-procedure.pdf |
| Result notification and reassessment information | You will be provided feedback and the result for your assignment on TAFESA Learn. You will be and given the chance to resubmit with required corrections only once.  Refer to the TAFE SA assessment policy for more information <https://www.tafesa.edu.au/apply-enrol/before-starting/student-policies/assessment> |

## Scenario

ITWorks has created a training department named ITWorks Training which is acknowledged as an industry training leader delivering nationally recognised and specialised courses. ITWorks Training is a private registered training organisation (RTO) based in Adelaide, South Australia with satellite offices in Melbourne and Perth.

Registered training organisations (RTOs) are those training providers registered by ASQA (or, in some cases, a state regulator) to deliver vocational education and training (VET) services.

RTOs are recognised as providers of quality-assured and nationally recognised training and qualifications.

ITWorks Training can:

* Deliver nationally recognised courses and accredited Australian Qualifications Framework (AQF) VET qualifications,
* Apply for Australian, state and territory funding to deliver vocational education and training.

ITWorks Training offers qualifications at the following levels:

* Certificates I, II, III and IV
* Diploma
* Advanced Diploma
* Vocational Graduate Certificate
* Vocational Graduate Diploma.

ITWorks Training has a dedicated network system which is used by the RTO to access internet services. ITWorks Training has given access to staff and students to internet services through a dedicated network.

ITWorks Training has around 40 staff members and 150 students who use the network regularly.

Hackers have attacked the ITWorks Training systems and have stolen the personal data of the staff and students. ITWorks Training has recovered the data and restored the system to normal operations.

ITWorks Training had developed some data security policies / procedures prior to the cyber-attack:

* ITWorks-Information-Classification-and-Handling-policy.docx
* ITWorks-confidentiality-policy.docx
* ITWorks-data-protection-policy.docx
* ITWorks-backup-procedure-policy-procedure.docx
* ITWorks-Log-ICT-Service-Requests-procedure.pdf
* ITWorks-email-usage-policy.docx

ITWorks Training is now aware that a cyber attack can happen in multiple ways. The most commonly encountered cybersecurity risks by ITWorks Training are:

* Phishing attack
* Hacking
* Ransomware

ITWorks Training is also aware of various ways to resolve cyber-attacks including the following:

* Staff should be careful when opening emails from an unauthorised source which ask for a response
* Install a good anti-virus system
* Turn on spam filter for messages and emails
* Install a network firewall
* Install data access security

ITWorks Training needs to develop cybersecurity policies and procedures. The previous policies and procedures don’t cover most of the information due to which the cyberattack happened.

You have joined ITWorks Training as an IT expert and policy developer. You need to review the existing cybersecurity policies and complete the following activities:

## Task 1: Identify cybersecurity threats and trends

Question 1

In this activity, you need to develop a report on threats to the organisational and trends associated with cybersecurity.

Review the scenario and complete the following:

* Introduction
  + Discussing the current level of awareness in workplace
* Cybersecurity threats
* Ways to deal with the threats
* Cybersecurity trends
* List existing cybersecurity practices
* Conclusion

Use the template provided below to provide a detailed review of the current situation for your manager.

Once completed upload Task 1 to LEARN for marking.

|  |
| --- |
| **Template 1: Identify cybersecurity threats and trends** |
| **Introduction (approx. 50 words)**  The report is to review and build on the current policies and procedures to mitigate and eliminate possibilities of attacks to ITWorks IP. The current ITWorks awareness of cybersecurity is reasonable as they have steps that were implemented prior to the attack that had outlined basic steps to reduce chances of attacks. |
| **Cybersecurity threats explaining what they are and list a potential impact on the workplace for each (approx. 100 words)**  A phishing attack is a type of attack that is sent through communication channels such as emails and SMS. These attacks pretend to be from a trusted sender to trick the victim into clicking a link that is then used to steal sensitive information such as emails, passwords, and bank details. Phishing attacks have the potential to allow an unauthorized person to gain access to company services, documents, and data.  Hacking is an attack that exploits vulnerabilities in hardware or software to gain unauthorized access to systems. The impact of hacking is similar to phishing in that attackers can gain access to systems, but it goes further in that they can potentially gain root access instead of just the access level of the user whose information was phished.  Ransomware is a type of attack that encrypts all files on a device, rendering it unusable. Malicious actors will then demand a ransom payment in exchange for the decryption key. The main impact of ransomware is the loss of all system files, especially in cases where multiple devices are connected through a network. This creates a possibility for multiple devices to be affected through a single attack. |
| **Discuss 3 ways to resolve cybersecurity threats (approx. 50 words)**   1. Back up: Have a form of backup for staff. OneDrive is a good option, or a company server can be used. 2. Mandate up-to-date: Force computers to update their operating systems and antivirus software. Make sure that any other software used is up to date with the latest security patches. 3. Strong password policies: Force staff to create strong passwords when making accounts. Implement password managers that can generate strong passwords automatically. |
| **Discuss 2 techniques to resolve the phishing attack (approx. 50 words)**   1. Have all work go emails through a email gateway if they are from an unknown domain prior to the recipient receiving it. The check makes sures all links are legitimate. 2. Train staff so they know what phishing emails look like, making sure they don’t have obvious spelling errors, links look legitimate, emails are sent from people/companies you expect. |
| **Discuss 2 techniques to resolve hacking (approx. 40 words)**   1. Make sure software and firmware is up to date and the latest security patches are installed. 2. Use air gapped networks in areas where really high security is necessary, using gateways to access the networks |
| **Discuss 2 techniques to resolve Ransomware (approx. 60 words)**   1. Have regular backups of all devices. 2. Use and keep up to date antivirus software. |
| **Discuss 2 cybersecurity trends (approx. 20 words)**  Social engineering  Phishing |
| **5 current cybersecurity policy / procedures**   1. ITWorks-Information-Classification-and-Handling-policy.docx 2. ITWorks-confidentiality-policy.docx 3. ITWorks-data-protection-policy.docx 4. ITWorks-backup-procedure-policy-procedure.docx 5. ITWorks-Log-ICT-Service-Requests-procedure.pdf |
| **Outcome of report (approx. 50 words)**  In general, ITWorks has a good cybersecurity policy, but there are still areas for improvement. The main area for improvement is ensuring that staff members have a good understanding of what scams and phishing attacks look like. The policies should also address keeping passwords secure and ensuring that all software and firmware are updated. |

## Task 2: Review and update the company policy / procedures

Management believe it would be beneficial to create a specific cyber policy for ITWorks Training. They have sourced a generic policy to speed up the development process. Address the tasks below to finalise a complete cyber security policy for ITWorks Training.

Question 2:

* Using the ITWorks-generic-security-policy.docx as a guide update the current ITWorks-security-policy.docx to improve the risk mitigation strategies.
  + Find the missing 16 points and add them to the new policy.
  + Save the completed policy file name as ‘ITWorks-cyber-security-policy’
  + Once completed upload Task 2 to LEARN for marking.

Protect personal and company devices:

* Keep all devices password protected.
* Choose and upgrade a complete antivirus software.
* Ensure they do not leave their devices exposed or unattended.

Manage passwords properly procedure:

* Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
* Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
* Change their passwords every two months.

Additional measures:

* Change all account passwords at once when a device is stolen.
* Report a perceived threat or possible security weakness in company systems.
* Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
* All newly discovered threats will be emailed out to staff.
* Avoid accessing suspicious websites.

Our [Security Specialists/ Network Administrators] should:

* Install firewalls, anti malware software and access authentication systems.
* Arrange for security training to all employees.
* Inform employees regularly about new scam emails or viruses and ways to combat them.
* Revoke rights for third party vendors upon completion of work with organisation.
* Ensure The Principle of Least Privilege is in place for all users.

## Task 3: Promoting workplace cyber security

Question 3

You need to prepare and record a 3 – 5-minute training presentation based on previous activities to educate ITWorks Training department staff.

You must include the following in your presentation:

* Prepare at least 7-10 pptx slides
* Introduction – Outline reason for training
* Deliver cybersecurity policies and procedures update
  + - ITWorks-cyber-security-policy (updates to policy / procedures)
* List 5 ways for each dot point below to avoid cybersecurity threats:
  + Phishing attack
  + Hacking
  + Ransomware
* List 5 ways how avoid risk to cybersecurity (best practices)
* Conclusion

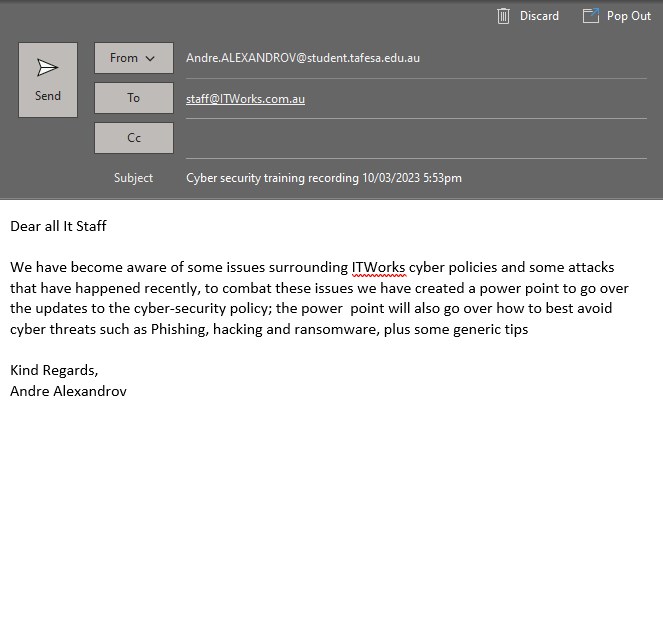
Save the recording as cyber-training.

Question 4

Word an email which you will send out to all staff, which needs to include:

* Subject: Attention All: Cyber security training recording (specify a date and time it was recorded)
* Body: Ensure an outline of training recording you had created in the above task is included within the body

Note: The email does not need to be sent, only created and a screen capture inserted in this document belows:



Question 5

Which would be a more effective timeframe to perform training to ensure staff are up to date with the latest Cyber threats?

* Once every 6 months or
* Once per 1 year or
* Once every 2 years
* 6 months

List 2 security points that would need to be updated regularly:

* Passwords
* Software is up-to date

Question 6

Your manager thinks it would be beneficial to have a quick brainstorming session with several key colleagues to come up with 3 different ways to promote cyber security in the workplace.

Work in a small group of 2 – 3 people to complete the template below (external students will be assigned groups – please email your lecturer for details).

IMPORTANT: Use the [Student-Subject Forum](https://learn.tafesa.edu.au/mod/forum/view.php?id=1031644) to reach out to other students within the subject to form groups. This is done by either responding to a student posted request link or by creating your own post by clicking the ‘Add a new discussion topic’. If you get stuck, please contact your subject lecturer for assistance, they will add you to a group.

All communication needs to be recorded, kept and included with your assessment submission as an appendix which can be screenshots of either:

* Group emails or
* Group Teams (or alternative tool) text chat or
* Teams Recordings
* ***NOTE: All students need to actively contribute to the discussion by voicing opinions regarding project ideas etc (minimum of two – emails or posts or text entries in Teams meetings)***

Each student needs to submit the completed template and recorded communications below.

Once completed upload all Task 3 files to LEARN for marking.

Must include the completed template below:

|  |  |  |  |
| --- | --- | --- | --- |
| **TRAINING PLAN** | |  |  |
| **TRAINING CONTACT** |  | **DEPARTMENT** | **DATE** |
|  |  | ITWorks Training |  |
| **GOALS / DESIRED OUTCOME** | | | |
|  | | | |
|  |  |  |  |
| **DATE / TIME TO IMPLEMENT** | **TASK - CYBER PROMOTION METHODS** | **DURATION** | **SIGNATURE / INITIALS** |
| 6th march | Cyber seminar | 30 min | AA |
| 10th march | Implement password managers training | 10 min | AA |
| 10th April | Phishing detection workshop. | 1 hour | AA |
|  |  |  |  |
|  |  |  |  |

## Paste team communication evidence below:

Graphical user interface, application, Teams

Description automatically generated

## Task 4: Manager catchup

The next step in this process is to have a quick chat / discussion (2 – 5 minutes max) with your manager (lecturer). Contact your Lecturer at least 24 hours in advance either verbally in class or via email to arrange a suitable time for this interview with your team member (fellow student).

If you are not attending a face-to-face interview (i.e. if you are studying this unit externally), you must ensure that you have access to a web camera and microphone and that the camera is turned on during the interview with your face clearly visible. Noting, the interview is not required to be recorded.

You must conduct the interview in a professional manner, ensuring that you use appropriate questions (open and closed) and demonstrate active listening techniques to acquire and confirm all the information listed in the questions below.

When undertaking the interview do not just read straight from the questions you addressed below. Use your own words when creating appropriate questions to gather the necessary information. Remember that in some instances you are confirming information that has already been provided in writing, but in other instances you are obtaining new information – ensure that you phrase your questions appropriately.

All parts are to be completed in the one interview.

You may record the interview or take written notes with pen and paper.

Recording or taking notes is not mandatory but is recommended for reference purposes.

Question 7

The focus of the discussion is for you to:

* Present insights from your review and training to required personnel and potential related impacts on the workplace