# Project assessment: Contribute to workplace security in a virtual environment

## Criteria

### Unit code, name and release number

BSBXCS404 - Contribute to cyber security risk management (1)

ICTICT451 - Comply with IP, ethics and privacy policies in ICT environments (1)

### Qualification/Course code, name and release number

ICT40120 - Certificate IV in Information Technology (3)

## Student details

### Student number

### Student name

## Assessment declaration

*Note: If you are an online student, you will be required to complete this declaration on the TAFE NSW online learning platform when you upload your assessment.*

This assessment is my original work and has not been:

* plagiarised or copied from any source without providing due acknowledgement.
* written for me by any other person except where such collaboration has been authorised by the Teacher/Assessor concerned.

### Student signature and Date

Version: 20211028

Date created: 1 June 2021

Date modified: 28 October 2021

For queries, please contact:

*Contact Details: Technology and Business Services SkillsPoint*

*Location: Parramatta*

© 2021 TAFE NSW, Sydney  
RTO Provider Number 90003 | CRICOS Provider Code: 00591E

This assessment can be found in the: [Learning Bank](https://share.tafensw.edu.au/share/access/searching.do?doc=%3Cxml%2F%3E&in=P7ac4831b-430a-4b8d-8b56-f7b32ed5b9cf&q=&type=standard&sort=rank&dr=AFTER)

The contents in this document is copyright © TAFE NSW 2021 and should not be reproduced without the permission of TAFE NSW. Information contained in this document is correct at the time of printing: 12 May 2022. For current information please refer to our website or your Teacher/Assessor as appropriate.

## Assessment instructions

Table 1 Assessment instructions

| Assessment details | Instructions |
| --- | --- |
| **Assessment overview** | The objective of this assessment is to assess your knowledge and performance in contributing to cyber security risk management and implementing and complying with IP, ethics and privacy policies and procedures. |
| **Assessment Event number** | 1 of 2 |
| **Instructions for this assessment** | This is a project-based assessment that assesses your knowledge and performance of the unit.  **Work on this Assessment *in a small team* – you must identify the roles played by each member of the team to receive marks**  This assessment is in four parts:   * Part 1: Plan strategies and protocols * Part 2: Consult with stakeholders * Part 3: Implement and monitor protocols and strategies * Part 4: Review protocols and strategies |
| **Submission instructions** | On completion of this assessment, you are required to submit it to your Teacher/Assessor for marking. Where possible, submission and upload of all required assessment files should be via the TAFE NSW online learning platform.  Ensure you have included your name at the bottom of each page of documents you submit.  It is important that you keep a copy of all electronic and hardcopy assessments submitted to TAFE and complete the assessment declaration when submitting the assessment. |
| **What do I need to do to achieve a satisfactory result?** | To achieve a satisfactory result for this assessment you must answer all the questions correctly.  If a resit is required to achieve a satisfactory result it will be conducted at an agreed time after a suitable revision period. |
| **What do I need to provide?** | * TAFE NSW student account username and password. If you do not know your username and password, contact your campus or service centre on 131601. * Computer or other device with word processing software and internet access * Writing materials, if required. |
| **What the Teacher/Assessor will provide** | * Access to this assessment and learning resources, including the student workbook and any supporting documents or links. * Organisational documentation, policies and procedures * Case studies * Relevant legislation, codes of practice and standards, which can be accessed via the internet * Cyber security information and data. |
| **Due date**  **Time allowed**  **Location** | Indicative time to complete assessment:   * In class: One hour * Out of class: Five hours. |
| **Supervision** | Part of this is an unsupervised, take-home assessment. Your Teacher/Assessor may ask for additional evidence to verify the authenticity of your submission and confirm that the assessment task was completed by you.  You may access your referenced text, learning notes and other resources. |
| **Assessment feedback, review or appeals** | In accordance with the TAFE NSW policy *Manage Assessment Appeals,* all students have the right to appeal an assessment decision in relation to how the assessment was conducted and the outcome of the assessment. Appeals must be lodged within **14 working days** of the formal notification of the result of the assessment.  If you would like to request a review of your results or if you have any concerns about your results, contact your Teacher/Assessor or Head Teacher. If they are unavailable, contact the Student Administration Officer.  Contact your Head Teacher/Assessor for the assessment appeals procedures at your college/campus. |

## Specific task instructions

### Scenario

You are working as an *Intern on rotation* at ***Game Environment***, a company that makes Serious Multiplayer Games for mobile devices and is branching into VR development.

On rotation, the hope is that you will be able to experience the various aspects of the business, and how they all fit together. You have previously worked in Game Design and on the games helpdesk, where players contact the company with problems.

Recently the company has been taken over by a large corporate called [Gelos Enterprises](https://share.tafensw.edu.au/share/items/d0b458dc-3922-409d-b1fe-9a2f785f4a38/0/GelosEnterprises.zip/index.html) (Gelos), which occurred just at the beginning of the global pandemic.

You have been appointed into a role that looks at how *Game Environment’s* protocols fit within the larger Gelos ecosystem, especially with regard to Cybersecurity, IP, Ethics and Privacy.

Gelos seems to understand the unique makeup of a game studio, and have tasked you with a project looking at:

* Issues around remote working for *Game Environment* employees, particularly involving protection of data and IP.
* Maintaining staff and player privacy in the new distributed environment, and
* Ensuring that Ethical behaviour plays a key role in staff operations.

Gelos’ management has recognised that, because of the adjustment to remote work options for all employees, they need to update their policies and procedures for offsite working. The updated policies and procedures will ensure that project teams are able to meet the Gelos business objectives of individuals and teams collaborating and engaging across the organisation while maintaining the correct level of ICT security to mitigate any cyber security risks. Gelos also has a business objective to ensure that all intellectual property (IP), ethics and privacy policies are in place and complied with by all employees and teams.

You have been asked to assist in the development and deployment of the protocols, policies and procedures necessary to ensure Gelos manages cyber security risks and complies with all relevant IP, ethics and privacy policies.

You have been supplied with the following documentation to assist you with this project:

* [Communication Procedure](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=55d8c18c-98ab-44da-a3ca-a904133bab2d) (GE\_Communication\_procedure.pdf)
* [Data Backup Policy](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=3db64d06-71bd-4eab-9110-8030142cbd61) (GE\_Data-Backup\_policy.pdf)
* [Data Protection Policy](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=825c6959-8447-4007-8839-2d9b69dbde74) (GE\_Data-Protection\_policy.pdf)
* [ICT Governance Policy](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=7041aeea-1a17-4f66-839d-f96f5c24d143) (GE\_ICT-Governance\_policy.pdf)
* [Intellectual Property Policy](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=1ab93cf6-0eed-498a-95a5-585a22042d54) (GE\_Intellectual-Property\_policy.pdf)
* [New staff IT induction kit](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=f5c55a22-6623-490f-b6d5-dc32e3790407) (GE\_New-Staff-ICT-Induction-Kit\_policy.pdf)
* [Privacy Policy](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=df50b7f8-f190-4a3c-aad0-83297b3c395d) (GE\_Privacy\_policy.pdf)
* [Standard Operating Environment](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=6d3ef7dc-b21a-41f9-bb56-006f7e9551b4) (GE\_SOE.pdf).

Gelos requires its management and employees to abide by the [ITPA (Information Technology Professional Association) code of ethics policy](https://www.itpa.org.au/code-of-ethics/).

Relevant legislation, regulations and codes of practice/industry standards can also be accessed from:

* [Federal Register of Legislation](https://www.legislation.gov.au/)
* [NSW legislation](https://legislation.nsw.gov.au/)
* [Australian Government Australian Signals Directorate](https://www.cyber.gov.au/)

## Part 1: Plan strategies and protocols

You have been asked for assistance in evaluating risks and protocols for staff working remotely. These will also assist with maintaining the IP, ethics and privacy policy procedures.

### Task 1 – Mitigate identified risks

Gelos has identified **four** cyber security areas of risk that need to be reviewed and assessed with the increase of staff moving to remote working.

The identified cyber risks are as follows:

1. A breach of *security and/or protocol compliance* **while working in a home office**.
2. A breach of *security and/or protocol compliance* **while working in a café**.
3. A breach of *cyber security guidelines* **when working on emails**.
4. A breach of *security and/or protocol compliance* **by a contractor**.

To successfully evaluate these identified risks, you will need to fill out a **Risk Register**. The Risk Register will be shared with relevant stakeholders for comment.

Make sure that you use clear and specific cyber security-related terminology, where appropriate.

Review the above risks and capture them in the **Game Environmemnt Risk Register** **template** provided, including:

* A description of the risk
* A Probability score – the likelihood of it occurring (1-5) using the Risk Matrix in the document
* An Impact score – the impact on the company if it did occur (1-5) using the Risk Matrix in the document
* A Severity score (Probability + Impact)
* Choose an appropriate strategy (Avoid/Reduce/Transfer/Accept)
* Indicate actions to be taken to mitigate the risk

**Additionally:**

1. For each of the four risks, what could be affected by this risk, including issues relating to IP, Ethics and Privacy.
2. How could you track the effectiveness of the risk management strategies. Suggest a benchmark or indicator you could use to assess how effective each strategy is.
3. What feedback processes would you recommend for providing warning of new risks?

### Task 2 – Develop a Standard Operating Procedure

To assist staff members, develop a **Standard Operating Procedure (SOP)** to define and improve the way Game Environment teams work in a virtual environment. This will also help support the maintenance and development of the studio’s IP, ethics, privacy policy and procedures.

Adapt the [Gelos SOP (Standard Operating Procedure) template](https://share.tafensw.edu.au/share/items/02285ff1-cfb2-4af4-b402-fdc23bf4bf11/0/?attachment.uuid=21046ae5-03d8-4725-9ccc-2a287e2eb913) to develop the SOP. Incorporate the **Game Environment** logo into the document to ‘rebrand’ it.

Your SOP must include the following:

Develop at least two protocols to help the team to complete work tasks and meet team objectives. They must include the following:

* 1. Discuss how the team should share information when collaborating in a virtual environment.
  2. Discuss how the team will follow organisational cyber security procedures when collaborating; include the first two recommended risk management strategies from your Risk Register
  3. Discuss how the *IP, ethics and privacy policy and procedures* are to be used to avoid infringing IP and privacy when working in a remote environment. You will need to refer to the procedures (links provided previously in this document)

Outline how the following will be monitored:

* 1. Cyber security risk, according to the two recommended risk management strategies.
  2. Whether or not personnel are adhering to the organisational IP, ethics and privacy policy and procedures.

## Part 2: Consult with stakeholders

Show evidence of consultation with **at least one other team** around your Risk Register and SOP. This may be in the form of screenshots of email responses, or you may wish to set up a Google Doc for responses, and take a screenshot, or a group chat.

As a result of this consultation, update your Risk Register documentation if required.

## Part 3: Implement and monitor protocols and strategies

You have been advised that there have been two incidents that have breached cyber security guidelines and the SOP for IP, Privacy and Ethics.

* The first incident involved an employee working remotely opening an attachment to a spam email, which had the potential to infect the *Game Environment* player database.
* The second incident involved an employee unknowingly disclosing personal player information in an email sent to an external party.

Determine whether staff members are complying with the approved cyber security risk strategies. Review the two incidents (outlined above) and complete the following:

1. Referring to your cyber security risk management strategies and SOP, analyse whether the employees complied with the strategies and where any non-compliance occurred.
2. Update the risk register with these incidents, completing a risk assessment for each.

## Part 4: Review protocols and strategies

You need to evaluate the effectiveness of the implemented risk management strategies against the benchmarks agreed to in Part 1, in particular, the strategies relating to the incidents mentioned in Part 3.

**What you need to do**

You will need to review the incidents and collaborate with your team members to:

* 1. evaluate the effectiveness of the risk mitigation strategies using the benchmarks that you identified in Part 1
  2. evaluate whether the implemented IP, ethics and privacy policies and procedures help prevent infringement and ensure compliance.
  3. develop recommendations to improve compliance
  4. update the Risk Register and SOP with the amended risk strategies and policies/procedures discussed

## Deliverables

1. Completed Risk Register containing all updates and relevant information
2. Standard Operating Procedure (SOP), amended where necessary
3. Evidence of consultation around the Risk Register and SOP

## Assessment Feedback

*NOTE: This section must have the Teacher/Assessor and student signature to complete the feedback. If you are submitting through the TAFE NSW online learning platform, your Teacher/Assessor will give you feedback via the platform.*

### Assessment outcome

Satisfactory

Unsatisfactory

**Assessor feedback**

Has the Assessment Declaration for this assessment event been signed and dated by the student?

Are you assured that the evidence presented for assessment is the student’s own work?

Was reasonable adjustment in place for this assessment event?

*If yes, ensure it is detailed on the assessment document.*

*Comments*:

### Assessor name, signature and date:

### Student acknowledgement of assessment outcome

*Would you like to make any comments about this assessment?*

### Student name, signature and date