2021 Subject & Assessment Guide

ICT Security Fundamentals

ICT30120

Certificate III in Information Technology

Game Development Foundations

Table of Contents

ICT Security Fundamentals

Units of Competency

The units of competency that are covered in this subject are as follows:

BSBXCS303 - Securely manage personally identifiable information and workplace information

Assessment processes and competency evidence requirements are described in the *Assessment Criteria* section below. If you have prior or other evidence against competency you should discuss this with your trainer.

Subject Overview

Overall Learning Outcomes

- Demonstrate responsible handling of personally identifiable information and workplace information.
- Apply industry best practices in the secure storage and sharing of personally identifiable information and workplace information.
- Apply information protection protocols.

Subject Description

This subject explores the secure handling and storage of personally identifiable information (PII) collected by an organisation as part of their business operations. You will learn about the national and international privacy legislation applicable to businesses, particularly as this applies to game studios. You will conduct a privacy impact assessment to uncover the impact privacy has on a game studio or game development team. Finally, you will research and use several digital tools and services that have been designed to strengthen organisational processes when dealing with PII or to assist you in strengthening your privacy processes and procedures.

Industry Relevance

Regardless of the size of an organisation, there are significant reputational and commercial benefits to be had by following good privacy practices. Consumers are more sensitive to all aspects of privacy, which is becoming increasingly critical to gain customer trust. When customers feel confident their personally identifiable information is handled securely by a company, they are much more likely to trust and use their products and services. It is also more effective and efficient to manage privacy risks proactively, rather than trying to retrospectively alter products or services to address any privacy issues that come to light. An understanding of the privacy legislation applicable to an organisation, and the impacts of privacy on the organisation is a critical part of any busines operation.

Assumed Knowledge

- Basic computer and internet literacy

Learning Components Guide

Your learning in this subject will be achieved through the following components. The study hours may vary.

Learning Component	Duration	Description
Classroom Activity	30 hours	Presentations, group work and tutorials
Individual Skills/Knowledge Development	5 hours	Self-paced practice exercises exploring Unity3D and basic skills in C#
Project Work	10 hours	Self-paced work developing a video game project, periodically checking-in with your trainer to show progress

Assessment Criteria

Assessment Description

Assessment Milestones

Please refer to your Class Schedule for actual dates on your campus

General Description

This assessment is comprised of several parts:

- a knowledge-based assessment,
- reviewing or writing workplace procedures on the handling of personally identifiable information (PII),
- conducting a privacy impact assessment,
- creating and securely storing a backup,
- setting up two-factor authentication, and
- securely storing strong passwords using a password manager.

Each assessment task is described below.

Knowledge-Based Assessment:

This consists of 8 short-answer tasks that will confirm your knowledge and understanding of the topics delivered as part of this course.

These questions are listed in Appendix 1, and can be completed via an online quiz at https://aie.instructure.com/ or answered and submitted in a MS Word document.

Workplace Information Handling Procedures:

Using the provided company procedures for securely handing PII you will review the procedures to ensure they are appropriate for a game studio and align with relevant legislation and industry best practice.

Your task will be to work through the Workplace Information Handling Procedures Worksheet, available on https://aie.instructure.com/, to review the PII handling processes and make updates to these as appropriate.

Privacy Impact Assessment:

For this task you will work through the Privacy Impact Assessment Worksheet to identify the potential impact of your business on individuals' privacy. As part of this process you will provide recommendations on how to manage, minimise, or eliminate the risk of non-compliance against data protection laws.

Securely Storing Backups:

You will be assessed on setting up a secure off-site data backup service, ensuring you apply the appropriate access permissions and security settings. You may choose any service to use for this part of this assessment (Dropbox, Google Drive, Sync, PCloud, etc.), but you must ensure the service has adequate security protocols in place and complies with the Workplace Handling Procedures you created as part of the assessment for this subject.

Once you have set up the data storage service, you will create a backup of any business related information (or any information used for any subject in this course) and store it securely using this service.

Setup Two-Factor Authentication:

You must turn on two-factor authentication for a service used during this course. This may be the data service you set up for this assessment, but it could also be any service you are using as part of this course (for example, Github, Trello, Discord, Gmail, etc.)

You must demonstrate the service configuration by submitting screenshots of either the confirmation screen after turning on two-factor authentication, or the login screen of the service requesting the two-factor authentication.

Securely Store Strong Passwords:

The final part of this assessment sees you creating an account or installing a password manager, and creating and storing at least one strong password.

Evidence Specifications

This is the specific evidence you must prepare for and present by your assessment milestone to demonstrate you have competency in the above knowledge and skills. The evidence must conform to all the specific requirements listed in the table below. You may present additional, or other evidence of competency, but this should be as a result of individual negotiation with your trainer.

Your Roles and Responsibilities as a Candidate

- Understand and feel comfortable with the assessment process.
- Know what evidence you must provide to demonstrate competency.
- Take an active part in the assessment process.
- Collect all competency evidence for presentation when required.

This table defines what you need to produce as evidence of competency.

Assessment Tasks & Evidence Descriptions
1. Knowledge Questions Evidence that includes: Demonstration of requisite knowledge through the completion of the Knowledge Assessment Tasks 1 – 8 (available on https://aie.instructure.com/ and in Appendix 1).
2. Applying Information Protection Protocols Evidence that includes: • Reviewing or writing processes and procedures relating to securely handling personally identifiable information and workplace information o This task may be demonstrated through the completion of the *Workplace Information Handling Procedures Worksheet* • Completion of a privacy impact assessment on data o This task may be demonstrated through the completion of the *Privacy Impact Assessment Worksheet*
3. Securely Storing Backups Evidence that includes: • The secure setup of an off-site data storage service • The creation of a data backup and secure off-site storage of that backup data, demonstrated at least once

4. Using Two-Factor Authentication
Evidence that includes:
• Demonstrated use of Two-Factor authentication for at least one business service or service used during this course.
 o Suggested services include:
  ▪ Github
  ▪ Trello
  ▪ Discord
  ▪ Gmail

5. Securely Storing Strong Passwords Evidence that includes:

- The setup of a password manager
  - Suggested password manager is BitWarden
- Creation of a strong password, at least once

Assessment Instructions for Candidate

METHOD OF ASSESSMENT

Assessment is a cumulative process which takes place throughout a subject. A 'competent' or 'not yet competent' decision is generally made at the end of a subject. Your assessment will be conducted by an official AIE qualified assessor. This may be someone other than your trainer. The evidence you must prepare and present is described

above in this assessment criteria document. This evidence has been mapped to the units of competency listed at the beginning of this document. Assessments will be conducted on a specific milestone recorded above in this assessment guide document.

ASSESSMENT CONDITIONS

Formative assessment takes place as your trainer observes the development of your work throughout the subject and, although the assessor is likely to be aware of the evidence you are submitting, it is your responsibility to be prepared for the interview where a competency judgement is made (summative assessment). Forgetting something, or making a small mistake at the time of the milestone assessment, can be corrected. However, the assessor may choose to assess other candidates who are better prepared and return to you if time permits.

Upon completion of the assessment you will be issued with feedback and a record of the summative assessment and acknowledge that you have received the result. If you are absent for the nominated assessment milestone (without prior agreement or a sufficiently documented reason) you will be assessed as not yet competent.

GRADING

The assessment you are undertaking will be graded as either *competent* or *not yet competent*.

REASSESSMENT PROCESS
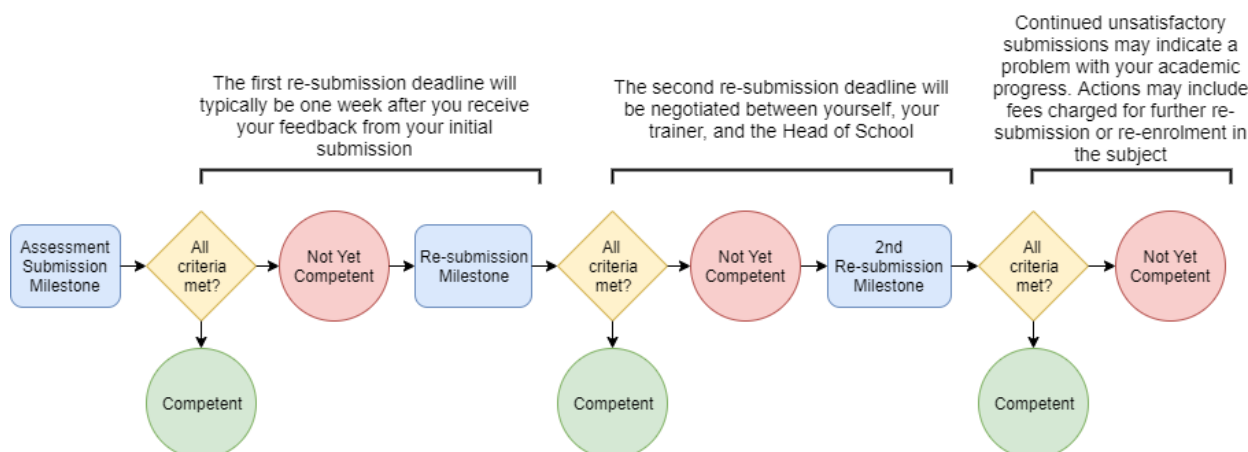
If you are assessed as being not yet competent you will receive clear, written and oral feedback on what you will need to do to achieve competence. You will be given a reassessment milestone no more than one (1) week later to prepare your evidence. If you are unsuccessful after your reassessment, you may be asked to attend a meeting with your Head of School to discuss your progress or any support you may need and further opportunities to gain competency.

REASONABLE ADJUSTMENTS

We recognise the need to make reasonable adjustments within our assessment and learning environments to meet your individual needs. If you need to speak confidentially to someone about your individual needs, please contact your trainer.

FURTHER INFORMATION

For further information about assessment and support at AIE, please refer to the assessment and course progress sections of your learner handbook.

Software

Core

Microsoft Word

Microsoft Word is industry standard word processing software, development by Microsoft and used throughout the course for creating documents and reports. Microsoft Word allows documents to be saved in *word* format, as well as several other standard document formats including *pdf*.

Learners will have access to Microsoft Word on campus but may also use alternate word processing software capable of loading and saving documents in *word* or *pdf* format.

- https://www.microsoft.com/en-us/education/products/office/default.aspx
- https://www.openoffice.org/
- https://www.google.com.au/docs/about/

7zip

7-Zip is a free and open-source file archiver, a utility used to place groups of files within compressed containers known as "archives". This utility program will be necessary to package your assessment files for submission.

- https://www.7-zip.org/download.html

Internet Browsers

A modern and up-to-date Internet browser is required to conduct research and access online tools and web sites. The most recent version of any mainstream Internet browser is required:

Chrome: https://www.google.com/intl/en_au/chrome/

Firefox: https://www.mozilla.org/en-US/firefox/new/

Edge: https://www.microsoft.com/en-us/edge

Appendix 1: Knowledge Assessment Tasks

Task 1 – Sensitive Data

What is sensitive data? Explain how to identify sensitive data in a workplace.

Task 2 – International Legislation

What are the 7 principles of the General Data Protection Regulation (GDPR)?

Task 3 – Data Breaches

When must an organisation or agency notify affected individuals and the Office of the Australian Information Commissioner (OAIC) according to Notifiable Data Breach legislation and Privacy Act 1988?

Task 4 – Data Protection

Explain why securing personally identifiable information (PII) is a critical data protection task.

Task 5 – Encryption

What are the uses of encryption?

Task 6 – Data Deletion

What is the difference between data deletion and data erasure?

Task 7 – Risks

What are the risks of communicating sensitive information via email and SMS?

Identify four (4) types of information that should never be shared via email or SMS?

Task 8 – Cloud Storage

What are four (4) risks and four (4) benefits associated with cloud storage?