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

COMPLIANCE GUIDE TEMPLATE	
Student Name	
Workplace/Organisation	Bounce Fitness
Date Prepared	
State/Territory	

Student's Work Role **Assessor instructions:** This must correspond to their work role in the job description accessed and reviewed for this task.	Network Operations Technician

To the student: For EACH of the 6 sets of policies and procedures you will assess for compliance, produce one copy of the following pages.

Assessor instructions: The student must relay information on the following policies and procedures:

- At **least three** existing policies and their corresponding procedures
  This refers to established, documented sets of rules that currently apply within the organisation's management of IP, ethics and privacy
- At **least three** potential policies and their corresponding procedures
  This refers to a draft of policies and procedures that apply to IP, ethics and privacy.

A. Policy/Procedure Information		
Name of Policy	Intellectual Property (IP) Policy	
Status **Assessor instructions:** This must correspond to one of the following options provided via the tick box: • Existing • Potential	☑ Existing	☐ Potential
Name of Relevant Procedure	IP Handling Procedures	

Types of Intellectual Property Covered by the Policy and Procedure (At least 3) **Assessor instructions:** This section must include three types of intellectual property covered by the identified policy and procedure, e.g. software, copyrighted content, trademarks, patents	i. Copyrighted materials ii. Trademarks iii. Patents
Corresponding Legislative Requirement **Assessor instructions:** This section must include at least one corresponding legislative requirement This refers to the legal documents that outline the framework and standards referenced by organisations for the development of their own policies and procedures for IP, ethics and privacy.	Responses can include: - Copyright Act 1968 (Cth) - Trade Marks Act 1995 (Cth) - Patents Act 1990 (Cth)
Reference or Source *Provide the link or name of the document where the policy and procedure was accessed from.* **Assessor instructions:** This section must include at least one reference or source for the policy and procedure document This refers to text such as a document title or link that directs a reader to the location of identified information.	ICTICT451_02_Intellectual Property, Ethics and Privacy Policies and Procedures document
Relevant Roles	

Assessor instructions: This refers to titles held by different personnel engaging in the compliance assessment that defines their expected responsibilities and duties in the workplace relevant to upholding IP, ethics and privacy in the workplace.	
Student's Role **Assessor instructions:** This must correspond to the role identified above.	Network Operations Technician: Ensure compliance with IP policies and procedures
Other Personnel's Roles **Assessor instructions:** This must correspond to the two other job descriptions provided in the assessment.	i. Network Security Analyst: Enforce IP protection measures on network infrastructure
	ii. Systems Administrator: Implement data protection protocols for IP stored on servers

B. Risk Assessment

Assessor instructions: This must correspond to the content of the latest organisational risk assessment documents accessed and reviewed for this task.

Risk (At least 2) **Assessor instructions:** This refers to instances of non-compliance to organisational policies and procedures for intellectual property that have the potential to negatively affect the flow of workplace operations.	**Likelihood of Risk** *Rare, Unlikely, Possible, Likely, Almost Certain* **Assessor instructions:** This refers to the probability that the identified risk will occur in the organisation's operations. The student's response must correspond to one of the following for each risk: - Rare - Unlikely - Possible - Likely - Almost Certain	**Consequence of Risk** *Negligent, Minor, Moderate, Major, Catastrophic* **Assessor instructions:** This refers to the impact the risk will have on the organisation when encountered. The student's response must correspond to one of the following for each risk: - Negligent - Minor - Moderate - Major - Catastrophic	**Risk Rating** *Low, Moderate, High* **Assessor instructions:** This refers to the evaluation of both the likelihood and consequence of a risk which determines the overall severity of the risk on the organisation's operations.	**Possible Corrective Actions** (Approximate word count: up to 30 words) **Assessor instructions:** This refers to an appropriate action that when taken minimises a risk's impact on the organisation. For example, a corrective action for the risk of 'outdated IP records' can be to establish an IP management system to regularly update records of the organisation's IP.
i. Phishing Attack	Possible	Major	Moderate	i. Conduct regular cyber security awareness training for employees ii. Implement email filtering solutions to detect and block phishing emails
ii.				

Unsecured Wi-Fi Network	Possible	Serious	Moderate	i. Implement strong encryption protocols for Wi-Fi networks ii. Enforce strict access controls and update Wi-Fi access credentials regularly

Add more rows as necessary.

C. Implementation Plan **Assessor instructions:** The student must outline one implementation plan for EACH identified policy and procedure to support organisational operations. An implementation plan refers to a set of step-by-step actions that shows the effective integration of IP, ethics and privacy policies and procedures in the workplace. Implementation plans support organisational operations by providing personnel with the necessary information and guidelines they can use in deploying policies and procedures in the workplace.				
Task Overview (Approximate word count: up to 30 words) **Assessor instructions:** This refers to a short statement summarising a key activity that the student must complete as a part of implementing the policy and procedure in the workplace.	**Expected Outcome** (Approximate word count: up to 30 words) **Assessor instructions:** This refers to the anticipated results of a successful execution of the outlined task.	**Resources Required** **Assessor instructions:** This refers to operational components that are essential to the implementation of policies and procedures in the workplace, e.g. manpower or tools. This must include the technology required to assess compliance, such as hardware and software for evaluation and documentation.	**Task Owner** *Indicate the work role or specific name of personnel, if available.* **Assessor instructions:** This refers to the name of a work role or the specific personnel who is responsible for completing the identified task.	**Timeline** **Assessor instructions:** This refers to a specific range of dates on which the task must be completed.
i.				

Meet with team leads to disseminate policy and procedure information for immediate implementation.	For example, if the task is to meet with team leads to communicate policy and procedure information, the corresponding expected outcome may be ‘Organisation-wide acknowledgement of the IP, ethics and privacy policies and procedures in the workplace.’	IT team, encryption tools	Network Operations Technician	Within two weeks
ii.				

Add more rows as necessary.

D. Policy/Procedure Effectiveness Monitoring Plan

Assessor instructions: The student must outline one effectiveness monitoring plan for EACH identified policy and procedure support organisational operations.

A monitoring plan refers to a set of performance standards and their corresponding values and methods of measure that show the effectiveness of policy and procedure deployment.

Monitoring plans support organisational operations by providing personnel with the necessary information and guidelines they can use in assessing project performance over the entire course of implementation.

Against IP Infringement

Areas for Monitoring (At least 2) **Assessor instructions:** This section must include at least two areas for monitoring. This refers to the specific tasks or areas of the personnel's performance during the planned implementation that show compliance with the policy or procedure.	**Performance Indicators** (At least 1 for each identified area) **Assessor instructions:** This must include at least one performance indicator for EACH identified area of monitoring. This refers to a quantifiable value that establishes the level of performance that must be achieved to establish that the policy/procedure implementation is effective.	**Method of Monitoring** (At least 1 for each identified area) **Assessor instructions:** This must include at least one method of monitoring for EACH identified area of monitoring. This refers to the specific approach used to identify the level of compliance demonstrated in the implementation of the identified policies and procedures.	**Schedule of Monitoring** **Assessor instructions:** This refers to when the identified area for monitoring will be evaluated. This can be: - Specific date, e.g. 26 July 20YY - An interval, e.g. after 3 months - Adverbs for frequency, e.g. monthly, quarterly
i. Employee compliance with IP policies.	Number of reported IP policy violations.	Regular audits and employee feedback.	Monthly
ii.			

Add more rows as necessary.

Against Privacy Infringement			
Areas for Monitoring (At least 2) **Assessor instructions:** This section must include at least two areas for monitoring.	**Performance Indicators** (At least 1 for each identified area) **Assessor instructions:** This must include at least one performance indicator for EACH identified area of monitoring.	**Method of Monitoring** (At least 1 for each identified area) **Assessor instructions:** This must include at least one method of monitoring for EACH identified area of monitoring.	**Schedule of Monitoring** **Assessor instructions:** This refers to when the identified area for monitoring will be evaluated. This can be: - Specific date, e.g. 26 July 20YY - An interval, e.g. after 3 months - Adverbs for frequency, e.g. monthly, quarterly
i. Data access logs and security incidents related to IP	Number of unauthorised data access attempts	Security software logs and incident reports	Weekly
ii.			

Add more rows as necessary.

END OF COMPLIANCE GUIDE TEMPLATE