Task 1 : Based on the cybersecurity strategy you developed with your group in EMCS 601, and the controls which you developed, your company now needs a policy for Cybersecurity.

[T1.1] Write the name of your company or organization ?

The name organization is Jeddah university.

[T1.2] Who would be the target audience for the policy?

The Jeddah University enterprise ITC Hierarchy program is delegated to the groups and individuals as defined below.

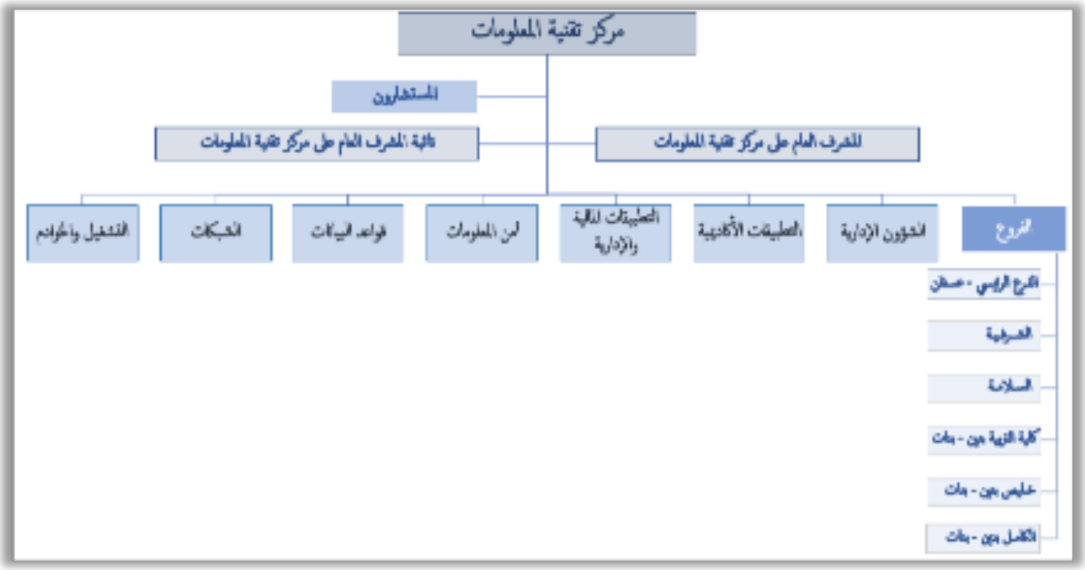


Figure 2: ITC Hierachry

[T1.3] Write an introduction to the policy. Who will authorize the Introduction?

Introduction:

Cybersecurity is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it.

Organization Profile

Digital transformation means the pursuit of the organizations' strategy, the development of innovative business and operating models, and flexibility by investing in technologies, developing talent, reorganizing operations and managing change to create an environment for customers, employees and stakeholders.

In the interest of Jeddah University to accomplish the digital transformation process, work has been done to develop the technical environment and create an updated structure in accordance with the strategic objectives of digital transformation in accordance with the Kingdom's 2030 vision, with the aim of creating and launching high- quality technologies for advanced services and applications that are made based on local and international standards.

Organization Key players

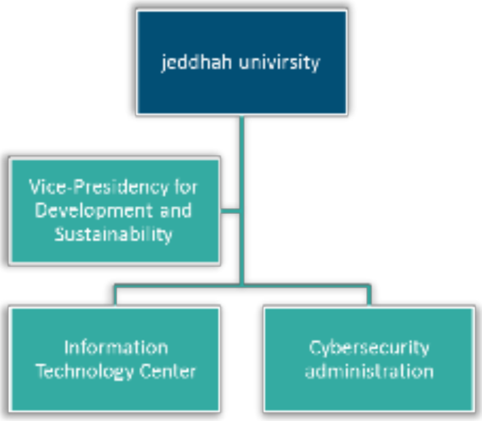

jeddhah univirsity
Vice-Presidency for Development and Sustainability
Information Technology Center
Cybersecurity administration

Figure 1: Organization Key players

Objective 1 : customer service .

Providing high-level customer service, customer satisfaction is one of the key performance indicators as we strive to improve service quality by investing in people competencies and continually improving processes and infrastructure.

Objective 2 : paperless online campus .

- Building information technology networks at the university, linking them to the global network, and supervising the improvement and development of network performance and speed and e-mail service efficiency.
- Striving to automate administrative procedures and work, make all electronic services available, and ensure their availability at all times and from anywhere.
- Developing the technical infrastructure and environment and applying best practices and methodologies in management and quality to raise operational efficiency.
- Providing and holding basic training programs on computer applications and its uses, as well as advanced training programs for databases, computers, and university systems and programs aimed at employees of the Authority, including academics and administrators.
- Keeping pace with the Kingdom's vision 2030 and achieving the goals of transformation 2020
- Transition to fully automated work (e-government) according to the latest technology
- Enhancing the concept of governance by applying the latest administrative tools that serve it.
- Ongoing awareness of the importance of technical change.
- Reaching the level of institutional excellence

Objective 3 : Policy measures to preserve data .

There are many policies applied and implementation of procedures , technical ,and procedural controls, which ensure their application through the technical solutions to information security, ensuring the continuity and integrity of the work of the information technology system at the University of Jeddah and protect the privacy of data and related information .Confidentiality has been achieved by implementing many procedures, including : if an employee wants to access the system, he will be allowed (5 times) attempts, more than that, the system will block him , and each employee has specific powers so that no employee can perform other than his responsibilities. The organization also obliges its employees to use strong and complex passwords, and enables them to use it for a specified period only, until they are forced to change it when the period expires, which increased the preservation of the confidentiality of information within the organization. The organization's systems are very important and sensitive, so we had to ensure the confidentiality of these systems and the information they contain, so none of the systems can be accessed except through the organization's network only. The production environment within the organization can only be accessed by authorized persons. To ensure the confidentiality of all the company's information, a (non- disclosure) document was prepared and signed by all employees. The organization also achieved integrity by developing and testing all its systems within the development and experimentation environment. The organization also applies a system (load balance) to ensure the work of all servers and devices with high efficiency and the continuation of their systems and information all the time. The organization is also keen to provide daily backup copies of its information, making it available when needed. The organization applies physical security measures to prevent unauthorized access to its property such as equipment, devices and servers. To ensure confidentiality, availability and integrity, the organization used an SSL certificate to ensure a secure connection between the user and the organization's Internet, and applied SSH port 22 encryptions between devices. It also provided anti-virus programs such as trend micro and firewall and used (systems control) to monitor all its systems.

• Signature-Based - The signature-based approach uses predefined signatures of well-known network threats. When an attack is initiated that matches one of these signatures or patterns, the system takes necessary action.

- Anomaly-Based - The anomaly-based approach monitors for any abnormal or unexpected behavior on the network. If an anomaly is detected, the system blocks access to the target host immediately.

- Policy-Based - This approach requires administrators to configure security policies according to organizational security policies and the network infrastructure. When an activity occurs that violates a security policy, an alert is triggered and sent to the system administrators.

In our network organization we use Network Security Devices :

- Firewalls: PREVENTION
- NIDS (network intrusion detection systems): DETECTION
- NIPS (network intrusion prevention systems): PREVENTION

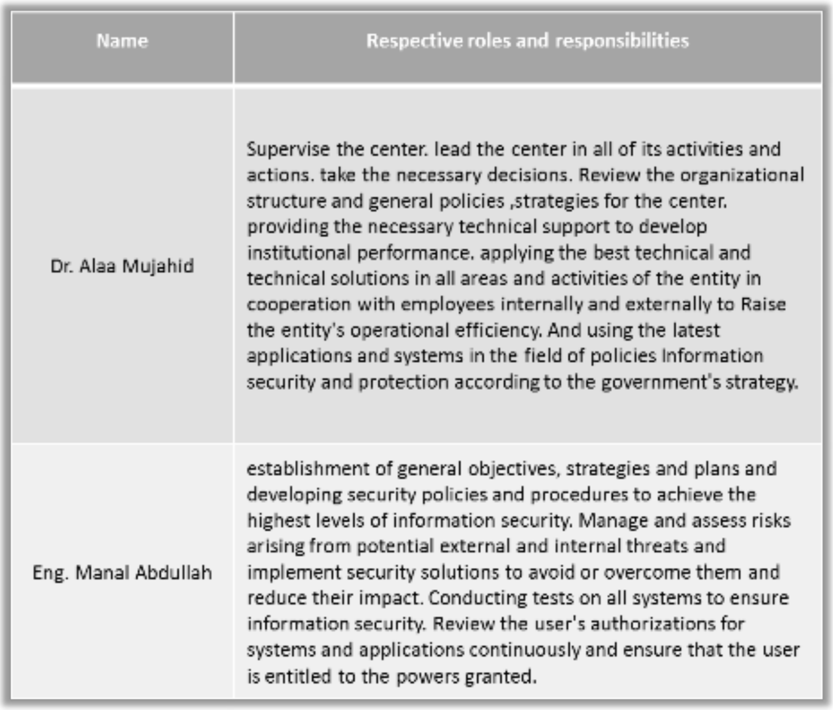
Objective 4 : consequence and exception process.

1. Each user has specific roles and responsibilities in the system.
2. Sensitive and important systems can only be accessed through the organization's network.
3. Include accountability, showing who has accessed data, when and from which device.
4. Server and network rooms are controlled by closed doors , the use of a CCV system , and the use of card reader .
5. Physical security measures To protect the organization's equipment.
6. The production environment can only be authorized by authorized persons.

Objective 5 : thank the reader and provide a seal of authority.

I thank you in advance for your support , as we all do our best to create a secure environment and to fulfill our mission , we highly appreciate you being a part of our success.

Who will authorize the Introduction?



Name	Respective roles and responsibilities
Dr. Alaa Mujahid	Supervise the center. lead the center in all of its activities and actions. take the necessary decisions. Review the organizational structure and general policies ,strategies for the center. providing the necessary technical support to develop institutional performance. applying the best technical and technical solutions in all areas and activities of the entity in cooperation with employees internally and externally to Raise the entity's operational efficiency. And using the latest applications and systems in the field of policies Information security and protection according to the government's strategy.
Eng. Manal Abdullah	establishment of general objectives, strategies and plans and developing security policies and procedures to achieve the highest levels of information security. Manage and assess risks arising from potential external and internal threats and implement security solutions to avoid or overcome them and reduce their impact. Conducting tests on all systems to ensure information security. Review the user's authorizations for systems and applications continuously and ensure that the user is entitled to the powers granted.

[T1.4] Compose a policy statement addressing Management, Operational and Technical roles and responsibilities.

Control Family	Class	Assets	Risk	List of Controls
Program Management	Management	Systems and servers	Systems disable or work wrongly	Use the systems/servers performance monitoring system, Alert is made when an error occurs
			Increase the load on a specific system or server and cause it to be disabled	Use of a load balancing system.
Awareness and Training	Operational	employees	This will have a direct implication on quality of work and Lack of awareness of employees in responding to risks	supervising the set controls and enabling training for staff
				Make sure it includes guidelines for staff under various risk levels
Contingency Planning	Operational	Data and information	Loss or tampering with important data and information	Provide daily backup copies of information.
			Unauthorized access	Each user has specific roles and

Access Control	Technical	Sensitive and important systems and data		responsibilities in the system.
			DDoS Attacks on the organization's network and Unauthorized access	Sensitive and important systems can only be accessed through the organization's network.
			Password Spraying and dictionary attack	Require employees to use strong and complex passwords and oblige them to change it after a specified time.
Audit and Accountability	Technical	Data	Unauthorized access , then change or delete data	Include accountability, showing who has accessed data, when and from which device.

[T1.5] Compose an enforcement clause.?

- The production environment can only be authorized by authorized persons.
- Must provide daily backup copies of information.
- Preparing a non-disclosure document for the organization's data and information, and the employees' signature on it.
- Physical security measures to prevent unauthorized access to the organization's property (equipment, devices, servers ...).
- Require employees to use strong and complex passwords and oblige them to change it after a specified time.

[T1.6] Compose an exception clause

- Allow a certain number (5 times) to access the system, more than that! The user will be blocked.
- Each user has specific roles and responsibilities in the system.
- Sensitive and important systems can only be accessed through the organization's network.

- Systems development and testing takes place in the development and experimental environment.
- Using of an SSL certificate to ensure a secure connection between the user and the organization’s Internet.
- Using SSH Port 22 encryption between devices.
- A high degree of security in the organization's hardware and servers by providing anti-virus programs such as the trend micro and firewall.
- Use the systems performance monitoring system.

[T1.7] Determine which terms should have definitions.

SSL certificate (Secure Sockets Layer)
Secure Socket Layer, which is an Internet protocol for securing the transfer of data between a user's browser and the site he is visiting.

NIDS (network intrusion detection systems)

Intrusion Detection Systems is a program and / or device designed to detect unwanted access to a computer system or attempt to disrupt this system in general and to tamper with it, through a work network, such as the Internet. Network-based Intrusion Detection System (NIDS)

NIPS (network intrusion prevention systems)

Network-based intrusion prevention systems (NIPS): monitors the entire network for suspicious traffic by analyzing protocol activity.

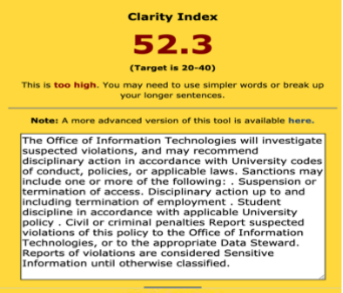
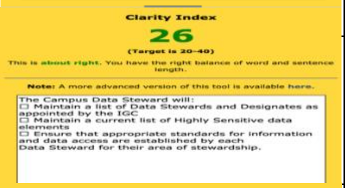
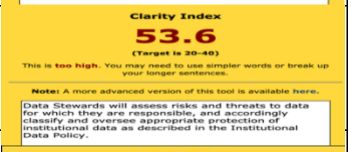
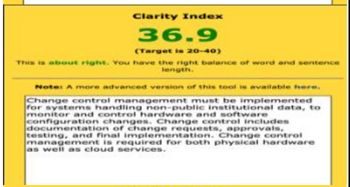
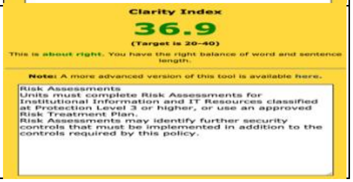
Task 2 - Go to EDUCAUSE website (https://www.educause.edu/focus-areas-and-initiative s/policy-and-security/cybersecurity-program/resource s/information-security-guide/security-policies/inform action-security-policy-examples) and from Information Security Policy Examples select three policies from the same category Note: Export the selected policies into three separate documents (pdf or Word format)

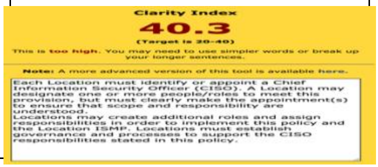
[T2.1] Read the documents and identify the policy components (Highlight on the documents with Comments).

[T2.2] Find where a standard, guideline, or procedure is embedded in the policy documents. (Highlight on the documents with Comments)

General Information Security Policies	DOC 1	DOC 2	DOC 3
	Information security policy	Security Policy IT Security & Policy Office.	

[T2.3] Use the U.S. Army's Clarity Index to evaluate the ease of reading of these documents [One bad and One good paragraph from each document]

DOC	BAD / GOOD	PARAGRAPHS	CLARITY INDEX
DOC 1	BAD PAGE 4 SECTION6	The Office of Information Technologies will investigate suspected violations, and may recommend disciplinary action in accordance with University codes of conduct, policies, or applicable laws. Sanctions may include one or more of the following: . Suspension or termination of access. Disciplinary action up to and including termination of employment . Student discipline in accordance with applicable University policy . Civil or criminal penalties Report suspected violations of this policy to the Office of Information Technologies, or to the appropriate Data Steward. Reports of violations are considered Sensitive Information until otherwise classified.	 Clarity Index 52.3 (Target is 20-40) This is too high. You may need to use simpler words or break up your longer sentences. Note: A more advanced version of this tool is available here. The Office of Information Technologies will investigate suspected violations, and may recommend disciplinary action in accordance with University codes of conduct, policies, or applicable laws. Sanctions may include one or more of the following: . Suspension or termination of access. Disciplinary action up to and including termination of employment . Student discipline in accordance with applicable University policy . Civil or criminal penalties Report suspected violations of this policy to the Office of Information Technologies, or to the appropriate Data Steward. Reports of violations are considered Sensitive Information until otherwise classified.
	GOOD PAGE 1 SECTION 2.2	Campus Data Steward The Campus Data Steward will: Maintain a list of Data Stewards and Designates as appointed by the IGC .Maintain a current list of Highly Sensitive data elements .Ensure that appropriate standards for information and data access are established by each Data Steward for their area of stewardship.	 Clarity Index 26 (Target is 20-40) This is about right. You have the right balance of word and sentence length. Note: A more advanced version of this tool is available here. The Campus Data Steward will: □ Maintain a list of Data Stewards and Designates as appointed by the IGC □ Maintain a current list of Highly Sensitive data elements □ Ensure that appropriate standards for information and data access are established by each Data Steward for their area of stewardship.
DOC 2	BAD PAGE6 SECTION2	Data Stewards will assess risks and threats to data for which they are responsible, and accordingly classify and oversee appropriate protection of institutional data as described in the Institutional Data Policy.	 Clarity Index 53.6 (Target is 20-40) This is too high. You may need to use simpler words or break up your longer sentences. Note: A more advanced version of this tool is available here. Data Stewards will assess risks and threats to data for which they are responsible, and accordingly classify and oversee appropriate protection of institutional data as described in the Institutional Data Policy.
	GOOD PAGE7 SECTION2	Change control management must be implemented for systems handling non-public institutional data, to monitor and control hardware and software configuration changes. Change control includes documentation of change requests, approvals, testing, and final implementation. Change control management is required for both physical hardware as well as cloud services.	 Clarity Index 36.9 (Target is 20-40) This is about right. You have the right balance of word and sentence length. Note: A more advanced version of this tool is available here. Change control management must be implemented for systems handling non-public institutional data, to monitor and control hardware and software configuration changes. Change control includes documentation of change requests, approvals, testing, and final implementation. Change control management is required for both physical hardware as well as cloud services.
DOC 3	GOOD PAGE14 SECTION6.1.1	Risk Assessments Units must complete Risk Assessments for Institutional Information and IT Resources classified at Protection Level 3 or higher, or use an approved Risk Treatment Plan. Risk Assessments may identify further security controls that must be implemented in addition to the controls required by this policy.	 Clarity Index 36.9 (Target is 20-40) This is about right. You have the right balance of word and sentence length. Note: A more advanced version of this tool is available here. Risk Assessments Units must complete Risk Assessments for Institutional Information and IT Resources classified at Protection Level 3 or higher, or use an approved Risk Treatment Plan. Risk Assessments may identify further security controls that must be implemented in addition to the controls required by this policy.

DOC 3	BAD PAGE9 SECTION2.1	Each Location must identify or appoint a Chief Information Security Officer (CISO). A Location may designate one or more people/roles to meet this provision, but must clearly make the appointment(s) to ensure that scope and responsibility are understood. Locations may create additional roles and assign responsibilities in order to implement this policy and the Location ISMP. Locations must establish governance and processes to support the CISO responsibilities stated in this policy	Number of sentence = 4 Number of words = 71 Number of long words= 17 Clarity Index = 40  Clarity Index 40.3 (Target is 20-40) This is too high. You may need to use simpler words or break up your longer sentences. Note: A more advanced version of this tool is available here. Each Location must identify or appoint a Chief Information Security Officer (CISO). A Location may designate one or more people/roles to meet this provision, but must clearly make the appointment(s) to ensure that scope and responsibility are understood. Locations may create additional roles and assign responsibilities in order to implement this policy and the Location ISMP. Locations must establish governance and processes to support the CISO responsibilities stated in this policy.

[T2.4] How can you make the policy more readable?

DOCUMENTS	POLICY COMPONENTS	YES / NO
DOC1	Version control	Yes
	Introduction	Yes
	Policy heading	No
	Policy goals and objectives	No
	Policy statement	Yes
	Policy exceptions	Yes
	Policy enforcement clause	Yes
	Administrative notations	Yes
	Policy definitions	Yes
DOCUMENTS	POLICY COMPONENTS	YES / NO
DOC 2	Version control	Yes
	Introduction	Yes
	Policy heading	Yes
	Policy goals and objectives	Yes
	Policy statement	Yes
	Policy exceptions	Yes
	Policy enforcement clause	Yes
	Administrative notations	Yes
	Policy definitions	No
DOCUMENTS	POLICY COMPONENTS	YES / NO
DOC 3	Version control	Yes
	Introduction	Yes
	Policy heading	Yes
	Policy goals and objectives	No
	Policy statement	Yes
	Policy exceptions	Yes
	Policy enforcement clause	No
	Administrative notations	No
	Policy definitions	Yes

Proposed improvements for document		
DOC 1	DOC 2	DOC 3
The components are not used policy heading, policy goals and objectives .	The document not use policy definitions and policy statement no clear from the reader.	The document is not use is clear from the reader the policy exception and policy enforcement more in detail .