

Information Security policies and Procedures :-

Corporate policies:- Most organizations have a standard set of policies that govern the way they perform their business. There are at least 11 Tier 1 policies; this means that a policy is implemented to support the entire business or mission of the enterprise.

Corporate organization

Corporate policies

Employment	Employee Standard of conduct	Conflict of Interest	Procurement and Contracts	Employee Discipline
Workplace Security	Information Security	Corporate Communication	Records management	Asset classification

Organizationwide (TIER-1) policies :-

1. Employment Practices :- This is the policy that describes the processes required to ensure that all candidates get an equal opportunity when seeking a position with the organization. This policy discusses the organization's hiring practices and new employee orientation.
2. Standards of conduct :- This policy addresses what is expected of employee and how they are to conduct themselves when on company property, the representing

organization." Company management has the responsibility to manage enterprise information, personnel, and physical properties relevant to their business operations, as well as the right to monitor the actual utilization of these enterprise assets".

Conflict of Interest :- Company employees are expected to adhere to the highest standards of conduct.

Performance management :-

This policy discusses how employee job performance is to be used in determining an employee's appraisal. Information security requirements should be included as an element that affects the level of employee performance.

Employee Discipline :- When things go wrong, this policy outlines the steps that are to be taken. As with all policies, it discusses who is responsible for what and leads those individuals to more extensive procedures.

Information Security :- The bulk of the remainder of this book will address writing an effective information security policy.

Corporate Communications :- Instead of individual, topic specific policies on such items as voice-mail, e-mail, inter-office memos, (or) outside correspondence can be in a single policy on what is and is not allowed in organization.

Records management :- This policy was previously referred to as records retention but the concept has been refined.

This policy normally establishes :-

- * The record name
- * A brief description of the record
- * The owning department
- * The required length of time to keep the record.

Asset classification :- This policy was previously referred to as, classification categories and who is responsible for doing so. It normally includes the concept of employee responsibilities, such as the owner, custodian, and user.

The Asset classification Policy adds :-

- * The classification level
- * The owner's job title.

⇒ Topic Specific (Tier-2) policies :- There are also Tier-2 policies; these are topic-specific policies and address issues related to specific subject matter.

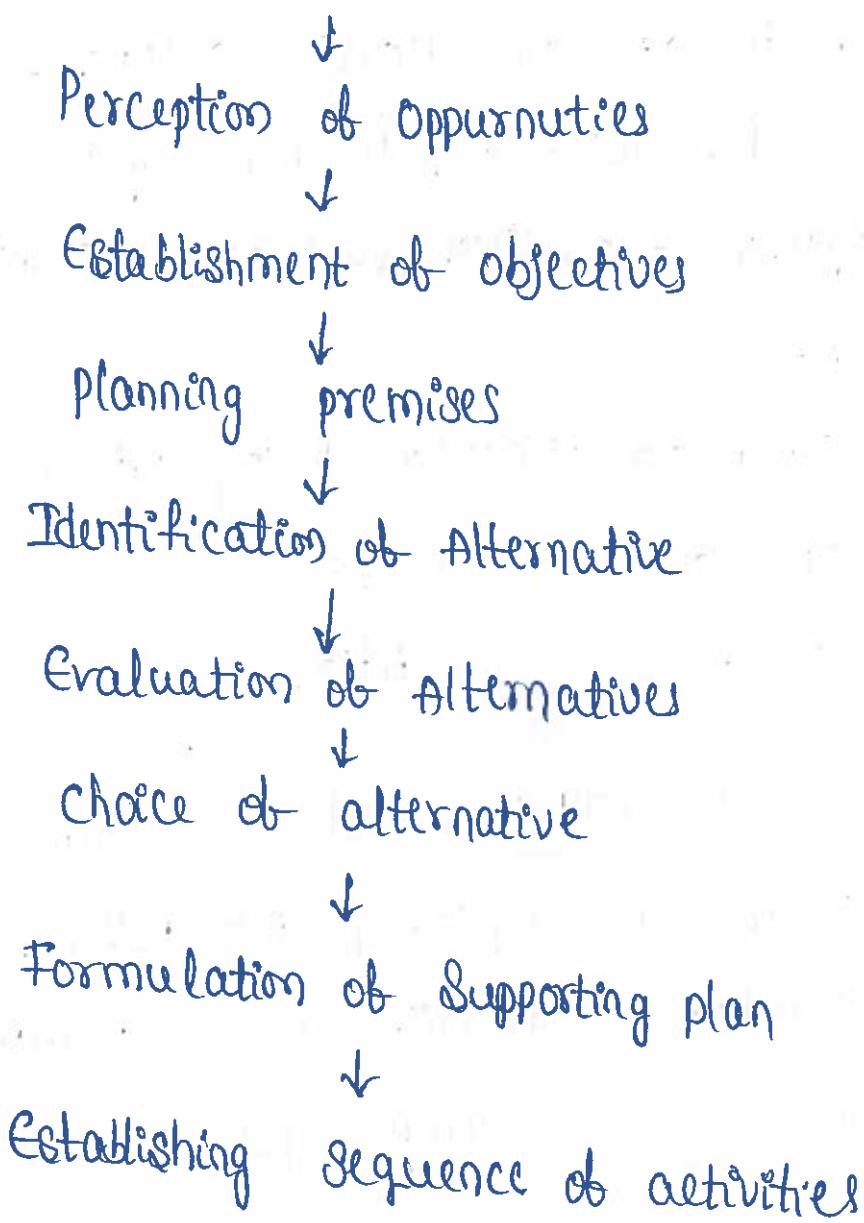
⇒ Application Specific (Tier-3) policies :- Tier-3 policies address the requirements for using and supporting specific applications.

* Process Management - planning :-

The process management plan is a document

document defining how a project is executed. The process owner creates the plan following inputs from the project team and the key stakeholders. It is a formal, approved document and that defines how the process is executed, monitored, and controlled.

The planning process :-



→ It may be a summary or a detailed document and may include baselines, subsidiary management plans and other planning documents.

This document is used to define the approach the project team takes to deliver the intended process management scope of the process.

⇒ Preparation developing policies :-

Policy development involves identifying need, gathering information, drafting, consulting and review.

→ The following steps summarise the key stages involved in developing policies.

1. Identify need :-

Policies can be developed :-

- * In anticipation of need (e.g. child protection policies should be in place once an organisation starts to work with children & young people)
- * In response to need (e.g. a policy position on a government strategy may be developed in response to a consultation paper).

2. Identify who will take lead responsibility :-

Do you have any legal responsibilities in this area? Is your understanding accurate and up to date?

Delegate responsibility to an individual working group.

Sub-committee or staff members, according to the expertise required.

3. Gather Information :-

Have other organisations tackled the same issue?
Are there existing templates (or examples) that you could draw on? Where will you go for guidance?

4. Draft policy :-

Ensure that the wording and length of complexity of the policy are appropriate to those who will be expected to implement it.

5. Consult with appropriate stakeholders :-

Policies are most effective if those affected are consulted and supportive and have the opportunity to consider and discuss the potential implications of the policy. Depending on whether you are developing policies to govern the internal working of the organisation (or) external policy positions, you may wish to consult for examples :-

- * Supporters
- * Staff and volunteers
- * Service users (or) beneficiaries.

6) Finalise / approve policy :-

Who will approve the policy? Is this a strategic issue that should be approved by the management Committee or is the committee confident that this can be dealt with effectively by staff?

→ Bear in mind that, ultimately, the management Committee is responsible for all policies and procedures within the organisation.

7) Implement :- How will the policy be communicated and to whom? Is training required to support the implementation among staff and volunteers? Should the organisation produce a press release?

8) Monitor, review, revise :-

What monitoring and reporting systems are in place to ensure that the policy is implemented and to assess usage and responses? On what basis and when will the policy be reviewed and revised?

⇒ Asset classification policy :-

Information Asset classification, in the context of information security, is the classification of information based on its level of sensitivity and the impact

to the university should that information be disclosed, altered or destroyed without authorisation.

→ The classification of information helps determine what baseline security controls are appropriate for safeguarding that information. All institutional information should be classified into one of three sensitivity tiers, 3 classifications.

* Tier 1 : Public Information

* Tier 2 : Internal Information

* Tier 3 : Restricted Information.

→ Information assets are classified according to confidentiality, integrity, and availability.

→ Each of these three principles of security is individually rated as low, moderate, or high.

Stages in policy development :-

* Identify need. Policies can be developed.

* Identify who will take lead responsibility

* Gather Information

* Draft policy

* Consult with appropriate stakeholders.

- * Finalise / approve policy
- * Consider whether procedures are required
- * Implement.

⇒ Developing Standards :-

There are 7 steps of the standards development process.

They are

1. Identify
2. Committee
3. Study
4. Consensus
5. Public review
6. Approve
7. Publish.

1. Identify :- First identify a need. This can be done by providers, patients or both. For instance, technology advancements in remote monitoring of health conditions may require new standards to reflect the new reality. Once a need is identified, project proposal to create a new standard (or to update an existing one, is put forward.

2. Committee :-

Standards are created or reviewed by the experts in the relevant field. They include researchers, care providers, patients and families who form into a technical committee.

3. Study :-

The technical committee conducts preliminary research and creates a draft outline of the new (or) revised standard. Much of this early work can be done remotely.

4. Consensus :-

Once a draft is written, technical committee members formally meet in person to approve a draft for public review. This consensus is required in order to progress any further.

5. Public Review :-

The next step to present the new (or) revised standards for public review. Anyone is welcome to provide feedback to improve its quality and ensure standards cover all relevant areas and perspectives.

6. Approve :-

After public review, the Standard goes back to the technical committee to make amendments if deemed necessary based on the feedback received. The committee then votes on the final version.

7. Publish :-

After the new or revised standards receives final approval from the technical committee, it is officially released. Health providers and systems may purchase it and incorporate it into their practice.

1. *What is the best way to get rid of the trash?*

2. *What is the best way to get rid of the trash?*

3. *What is the best way to get rid of the trash?*

4. *What is the best way to get rid of the trash?*

5. *What is the best way to get rid of the trash?*

6. *What is the best way to get rid of the trash?*

7. *What is the best way to get rid of the trash?*

8. *What is the best way to get rid of the trash?*

9. *What is the best way to get rid of the trash?*

10. *What is the best way to get rid of the trash?*

11. *What is the best way to get rid of the trash?*

12. *What is the best way to get rid of the trash?*

13. *What is the best way to get rid of the trash?*

14. *What is the best way to get rid of the trash?*

15. *What is the best way to get rid of the trash?*

16. *What is the best way to get rid of the trash?*

17. *What is the best way to get rid of the trash?*

18. *What is the best way to get rid of the trash?*

19. *What is the best way to get rid of the trash?*

20. *What is the best way to get rid of the trash?*