Security polices embedded in the information technology

The confidentiality,integrity,availability of the data is very important for the good governance Failure to adequately secure information increases the risk of financial and reputational losses. This information security policy outline approach to information security management.

It provides the guiding principles and responsibilities necessary to safeguard the security of the information systems. Supporting policies, codes of practice, procedures and guidelines provide further details. The main idea is basically to Provide the principles by which a safe and secure information systems working environment can be established for staff, students and any other authorized user. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits and penetration testing. Information security policy is nowadays a boom through which the organization should know why they are using the particular control. What is need of the particular control, whether the user is being informed or not. In many cases, the executives have no idea as to how information security can help their organization, so the main purpose of the [policy](https://advisera.com/27001academy/?p=2837&icn=paid-document-27001-information-security-policy&ici=top-policy-txt) is that the top management defines what it wants to achieve with information security.

The second purpose is to create a document that the executives will find easy to understand, and with which they will be able to control everything that is happening within the ISMS – they don’t need to know the details of, say, risk assessment, but they do need to know who is responsible for the ISMS.

