



IT SECURITY POLICY

Introduction:

Bayer recognizes that information and digitization are two cornerstones of Bayer's future, and that transformation into a digital, data-driven organization is key to Bayer's success.

This Policy forms the basis for an effective information security management for Bayer. It establishes basic requirements to ensure information security within Bayer, and provides a framework describing the duties and obligations for everyone handling Bayer's information including the assets associated with that information.

Roles and Responsibilities:

Roles and responsibilities are listed as under:

- Principles for Employees – Handling information with care and classify it in Internal, Restricted and Secret, Communication with caution, handling devices with care, clear workplaces and report suspicious incidents and loss of equipment.
- Reporting managers – Inform, train and promote awareness with the team, manage identities and ensure adequate security.
- Business Information Owners – Classify the information and nominate information classification caretakers
- Business owners of IT assets – IT asset classification, security by design, manage access, training and monitoring

Information Security Officer will head Information Security Management and enforce the implementation and operation of information security controls and processes.

Detailed policy:

The Bayer Corporate Policy 1435 on IT security can be referred for effective implementation of the policy.