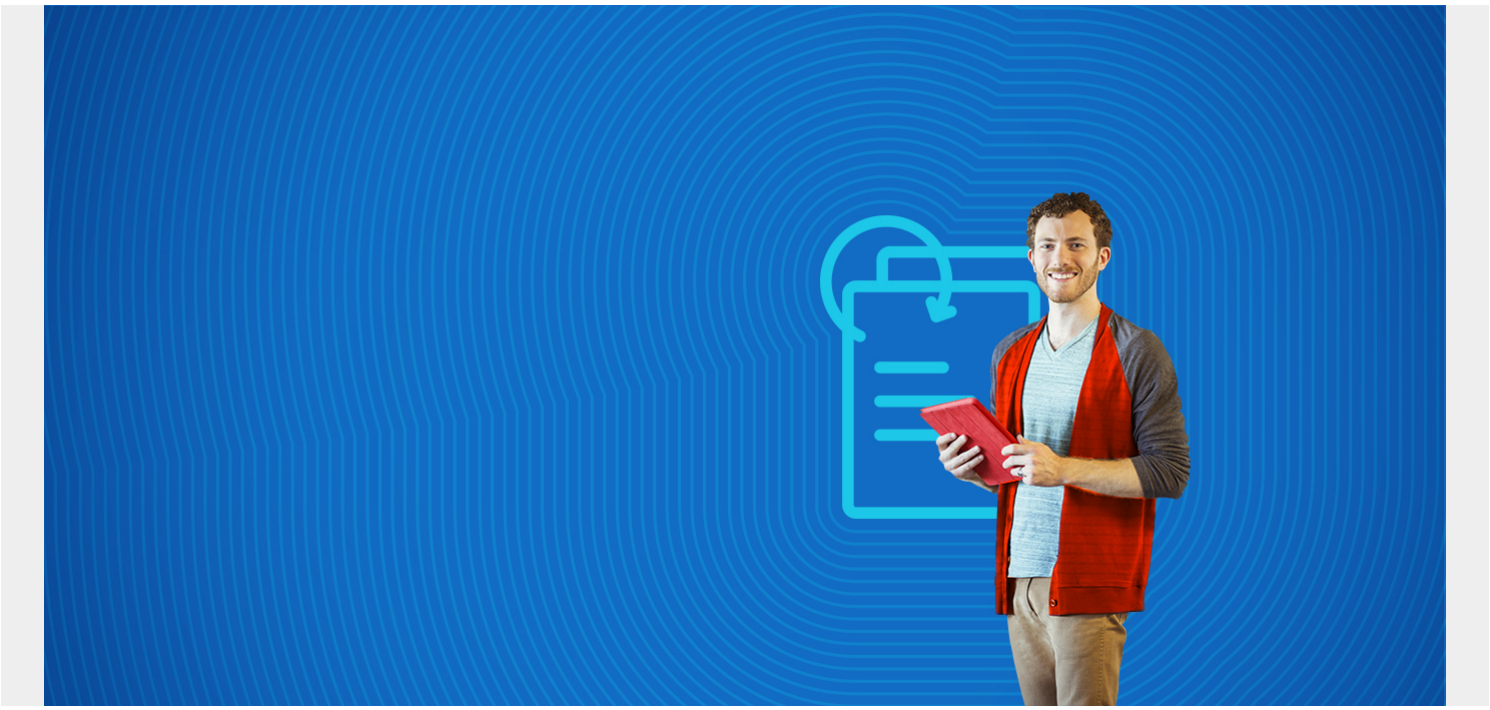
IT SECURITY POLICY: KEY COMPONENTS & BEST PRACTICES FOR EVERY BUSINESS



Back in 2017, The Economist declared that the world's most valuable resource is data. And a cursory look at the 2020 Forbes most valuable brands most valuable brands reveals that indeed tech runs the world now.

The downside of this is significant. There's now great pressure on companies to secure the information in their custody. Recent hacks involving SolarWinds, Twitter, and Garmin indicate that threats to information security continue to evolve, and all organizations have no option but to put in the legwork to establish and maintain required cybersecurity controls, whether their IT is on-premise, on cloud or outsourced.

From a governance perspective, an IT Security Policy is at the heart of this effort.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

Why do we need an IT security policy?

According to the ISO 27001:2013 standard, the objective of information security (InfoSec) policies is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

An IT security policy is a type of administrative control that communicates to all stakeholders involved in IT so that they understand what is expected of them in reducing the risks associated with information security. (It is not limited only to the security team.)

It also demonstrates the commitment by the highest level of leadership within the organization to

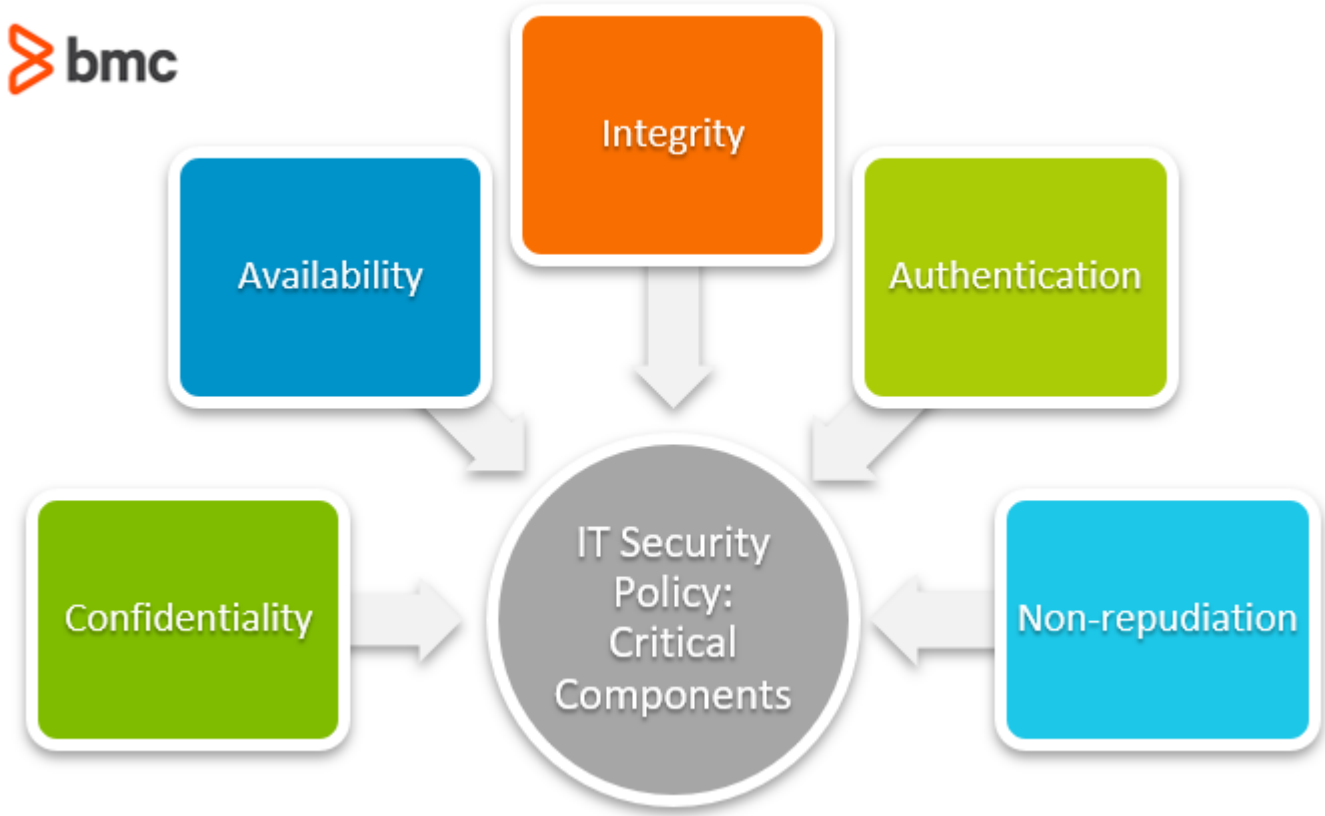
the ideals of the policy, therefore providing direction for the rest of the employees, suppliers, and other stakeholders.

(Explore the roles of Chief Information Security Officer and the security team.)

Whether at a strategic or tactical level, the IT security policy states 'why' the organization has taken a position to secure its IT systems. Most times, the rationale comes from:

- The value that the information held brings to the organization
- The need for trust from customers and stakeholders
- The obligation to comply with applicable laws

This is crucial from a governance perspective as it sets the tone for the design and implementation of IT security controls, and also institutes the relevant roles and responsibilities required for IT security to be managed effectively.



What's in an IT security policy?

At the core of any IT security policy is understanding and managing the risks to IT systems and data.

How the organization does this is by defining their chosen approach to achieving the required security posture or characteristics through relevant administrative, physical, and technical controls.

The ITIL® 4 Information Security Management practice spells out some of these security characteristics as follows:

- **Confidentiality:** The prevention of information being disclosed or made available to unauthorized entities.
- **Availability:** A characteristic of information that ensures it is able to be used when needed.
- **Integrity:** An assurance that information is accurate and can only be modified by authorized

personnel and activities.
- **Authentication:** Verification that a characteristic or attribute which appears or is claimed to be true is in fact true.
- **Non-repudiation:** Providing undeniable proof that an alleged event happened, or an alleged action was performed, and that this event or action was performed by a particular entity.

(Learn more about the CIA triad and additional security characteristics.)

The structure and size of an IT security policy varies from one organization to another, depending on their context:

- Some organizations deploy a large document with a lot of information on the controls.
- Others go for the simpler one-pager that references and points to other supporting documentation.

In terms of content, we can borrow from the CMMC model on what to include in your security policy:

- Purpose and scope
- Roles and responsibilities
- Establishment of procedures to meet the policy's intent
- Regulatory guidelines addressed
- Endorsement by management and dissemination to appropriate stakeholders
- Framework for periodic review and updating
- Reference to applicable sub-policies, procedures and controls

IT security policy best practices

Regardless of the structure, what matters in an IT security policy is that you're sending out a clear message to the entire organization and its stakeholders on what is required from an IT security standpoint.

The policy must be clear and unambiguous, with the right level of detail for the audience, and made easy to read and understand, especially for non-security experts.

Like other organizational-wide policies, you should create the IT security policy with the input of all relevant stakeholders. It would be imprudent for the IT management to develop a policy by themselves, without the buy-in of business users and external suppliers who they would expect to comply with it. Getting the input of stakeholders ensures broad based support in its implementation and compliance.

Alongside this is the need to communicate the policy to users and suppliers. The best bet for entrenching the IT security policy as the first line of defense against cybersecurity risks are these activities:

- Holding regular security awareness sessions for existing users.
- Establishing onboarding sessions for new users.
- Embedding policy requirements in supplier contracts.

A risk-based approach should be used for maintaining the IT security policy.

As your organization monitors and assesses the evolving risks to your IT infrastructure and data, you'll need to update this policy to ensure its relevance to the changing context.

In addition, measuring compliance to the IT security policy provides feedback to management on whether the policy itself is still effective and relevant. According to COBIT, some sample metrics related to policy compliance include:

- Number of incidents related to noncompliance with policy
- Percentage of stakeholders who understand policies
- Percentage of policies supported by effective standards and working practices

IT security policies aren't optional

An IT security policy that addresses, in particular, information security, is one of your most critical business policies. Without one, you risk your entire business.

Related reading

- BMC Security & Compliance Blog
- Introduction to Information Security Management Systems (ISMS)
- Cybersecurity: A Beginner's Guide
- Top IT Security, InfoSec & Cybersecurity Conferences