

## Case Study: Guiding Principles from MIT

---

### BACKGROUND

When creating a set of guiding principles, it can be helpful to examine examples from other organizations and to talk about the creation process those organizations used. Below is a set of guiding principles from Massachusetts Institute of Technology. For more information and a key to their terminology, visit their [guidelines](#) website.

### ARCHITECTURAL PRINCIPALS

This set of principles is written from a high-level perspective and with very few details. Even at such a high level, this set may not be ideal for organizations that value homogeneity and rapid deployment more so than standards based solutions. Others might want to add different bullet items needed to stress some of their local priorities, politics, or initiatives.

- Security: applications should ensure data and access security
- Ownership: clear and explicit ownership of enterprise data
- Leverage assets: leverage existing services and capabilities
- Accessibility: be aware of the needs of all users (location & disabilities)
- Real-time: Minimize latency of data updates
- Standards: promote consistency using standards

When the organization developed this simple set of principles they realized that these might be useful statements when communicating to other senior architects, but would not be sufficient for many project teams that they needed to communicate with and influence. In response, the organization developed another set of statements to inform and direct project teams across the organization.

The following statements apply now and into the future and are universally applicable to the organization's enterprise and departmental systems. However, these statements may not apply to your organization.

- There is a single shared campus network. (IP)
- The network should be considered public and unprotected.
- Unencrypted passwords MUST not go across the network.
- Application servers MUST not receive or store Kerberos passwords.
- Enterprise Applications SHOULD use the Campus single sign on mechanisms; Kerberos 5 and X509 Certificates.
- Departmental applications MAY wish to use these mechanisms.
- Applications that provide multiple authentication methods SHOULD provide individuals a choice, before a less secure option is presented to the user.
- The campus network does not have a perimeter firewall.
- Applications SHOULD use open specifications and standards where appropriate.

- University data SHOULD not be released or stored to a third party without an approved business reasons.
- The existence of an campus ID number does not indicate any membership in the campus community and MUST NOT be used for authorization decisions.
- The existence of a Kerberos name does not indicate any membership in the campus community and MUST NOT be used for authorization decisions.
- The existence of a X509 Certificate does not indicate any membership in the campus community and MUST NOT be used for authorization decisions.
- Access control SHOULD NOT be based on IP address.
- IP address of a computer is not a reliable way of determining the location of a machine.
- Applications SHOULD be able to be used across NATs.
- All protocols SHOULD be open and documented, so that they can be used in any computing environment.
- Members of the campus community are responsible for ensuring that their uses of the business data of the Institute are consistent with the Institute's policy on privacy of information
- Applications that transmit sensitive information including passwords over the network MUST encrypt the data to protect it from being intercepted by network eavesdroppers.
- Business data created at or obtained within the university belongs to the university, not to any particular function, unit, or individual.
- It is the responsibility of the designated custodian of a particular data collection to ensure data integrity, security, and accessibility to all who demonstrate need.
- The central data warehouse SHOULD be used for reporting where possible.
- Data feeds SHOULD come from the central data warehouse where possible.
- All people SHOULD have one unique public id, the campus ID number.
- All person records should carry the campus ID number.
- Critical and sensitive information SHOULD only be kept on machines that are professionally managed.
- Social Security number MUST NOT be used or stored.

The following statements refer to Enterprise systems:

- Authorization SHOULD be controlled by the Central Authorization System (Roles).
- A conceptual data model SHOULD be produced before any system is built or procured.

- Systems of Record SHOULD be established for all shared data.
- Usernames SHOULD be consistent across systems. Users should not be assigned a username different than their Kerberos principal.

In reading the preceding statements, notice that the topics are broader than simply authentication services. They are also a mixture of policy directives, technology directives, and in some cases pointed observations about the infrastructure.

MIT has a team of IT architects that consists of people from a variety of departments, including administrative and academic computing, the libraries, faculty, health services, the audit division, and others. The group met several times to develop the initial abstract principles and the more detailed statements. During the meetings everyone was encouraged to think about both policy and technology and systems that they knew about but had no direct responsibility for.