



Authentication policy

Version 1 – DRAFT / FINAL DRAFT / APPROVED	
Author: Gary@lsecT.com	
Policy approved by	Date approved
[Insert senior manager/director's name and job here]	[Insert approval date here]

Policy summary

Users of <ORGANIZATION>'s IT systems and networks must be positively identified to prevent access by unauthorized people. This policy mandates a range of controls to achieve that purpose.

Applicability

This is a standard corporate policy that applies throughout the organization as part of the corporate governance framework. It applies primarily to the design and management of our IT systems and networks.

Policy Detail

Background

Technical security controls that limit access to our computer systems, networks, program functions and data to legitimate, authorized users determine which users are attempting access according to the user IDs. Authentication controls ensure that each person is unambiguously associated with a unique user ID. If these controls are missing or fail, users may gain authorized access for example by entering another person's userID and guessing a weak password to logon to a system. Unless additional, stronger controls are enforced, the system will simply assume that the real user has logged on and will let the person do whatever the real user is allowed to do.

User authentication is therefore an extremely important computer security control. This policy lays out a number of security controls designed to strengthen user authentication and help prevent unauthorized access.

Policy axioms (guiding principles)

- A. Access to <ORGANIZATION>'s network, systems and data must be limited to authorized and authenticated users according to business need and information security policies.

Detailed policy requirements

1. <ORGANIZATION> systems must use secure logon processes where available.
2. Users must be identified and authenticated using mechanisms that meet the security requirements of specific systems:
 - Low-risk systems may use userIDs and passwords/PINs;

- Medium-risk systems may use multi-factor authentication using digital certificates or other tokens in addition to userID and passwords/PINs;
 - High-risk systems may require the use of even stronger authentication methods such as cryptographic tokens/smartcards or biometrics.
3. Every authorized user must have a unique identifier (userID) for their personal use in order to be able to trace activities logged by systems to the corresponding individual users. UserIDs must conform to naming standards and must not give any indication of the users' access rights e.g. contain words such as manager, supervisor or privileged.
 4. Where there is no alternative to using unique userIDs, a userID may be shared by a specific group of users for a specific purpose. Management must explicitly approve every shared userID. A single individual must be held personally accountable for use of each shared userID.
 5. UserIDs required for non-interactive automated system-to-system logons should be configured to block interactive use.
 6. Physical, logical and procedural controls must limit access to the <ORGANIZATION> network comprising the network links/connections, network nodes (including routers, firewalls, application servers, workstations and various other network-attached devices) and/or network services (such as file and print, HTTP/web and email services).
 7. Network access must be limited according to a combination of business requirements and information security policy requirements.
 8. Interconnections between <ORGANIZATION> and third-party networks must be explicitly authorized by the Information Security Manager.
 9. Users seeking access to <ORGANIZATION> networks must be authenticated at the initial point of entry into the network using unique userIDs and single- or multi-factor authentication (e.g. cryptographic security tokens or smartcards coupled with passwords, PINs and/or biometrics), according to the risks of unauthorized access. Unauthorized connections must be dropped ('default deny').
 10. User authentication devices (access control gateways, remote access tokens etc.) must be risk assessed and explicitly authorized by the Information Security Manager. Connections between <ORGANIZATION> and third party networks or systems must traverse authorized gateways.
 11. Connections between computer systems must be authenticated using secure methods approved by the Information Security Manager according to the level of security risk.

Responsibilities

- **Information Security** is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with various other departments and people, it is also responsible for specifying, designing and testing technical authentication and related controls such as the login process, data access rights, Public Key Infrastructure *etc.* and running the awareness, training and educational activities relating to information security issues.
- **Physical (Site) Security** is responsible for physical security controls in general, including authentication procedures for employees and visitors, issuance and recall of staff passes, control of physical keys, physical access controls, physical access monitoring *etc.* It is also responsible for running the awareness, training and educational activities relating to physical security issues.
- **IT Security Administration** is responsible for defining and operating processes relating to allocation and control of user IDs, user passwords *etc.*

- **IT Department** is responsible for developing and operating the technical controls associated with user authentication, logical access controls, data validation *etc.*
- **IT Help Desk** is responsible for assisting and advising employees in relation to electronic authentication.
- **All employees** are responsible for complying with this and other corporate policies at all times. They are personally accountable for their own activities on site and whilst using corporate IT facilities, and for the activities of any visitors or guests under their care.
- **Managers** (in conjunction with others as necessary) are responsible for funding, specifying, implementing and operating appropriate authentication and related controls in corporate IT systems under their remit, as well as other information security controls. This includes responsibility for periodically checking user access rights, allocation of system rights to user rôles, allocation of users to rôles, maintenance of appropriate divisions of responsibility and so forth. Managers are also responsible for ensuring that the associated processes are properly documented in formal procedures and that staff are made aware of their specific responsibilities through suitable awareness, training and educational activities.
- **Internal Audit** is authorized to assess the suitability and effectiveness of this and other corporate policies at any time.

Related policies

Relevance	Policy
Defines the overarching set of information security controls reflecting ISO 17799, the international standard code of practice for information security management	Information security policy framework

Contacts

For further information about this policy or information security in general, contact the Information Security Manager or Chief Information Officer. A variety of standards, procedures, guidelines and other materials supporting and expanding upon this and other information security policies are available in the organization’s Information Security Manual, on the corporate intranet and through the Information Security Manager. Local IT/information security contacts throughout the organization can also provide general guidance on the implementation of this policy - contact your line manager or the IT Help Desk for advice including the name of your local security contact.

Important note from IsecT Ltd.

This is a generic policy relating to a specific information security awareness topic. Because it is generic, it cannot fully reflect every NoticeBored customer’s requirements – in particular, it refers to specific departments and groups of staff, and references other policies that may or may not presently exist in your organization. It is not legal advice. It is unlikely to be complete, accurate and suitable to your specific organizational context without customization. *Caveat emptor.*