



## INFORMATION SYSTEMS POLICY

TITLE <b>PASSWORD / AUTHENTICATION PROTECTION POLICY</b>		CONTROL NUMBER <b>ISPOL-021-002</b>	EFFECTIVE DATE <b>June 1, 2004</b>
OWNER Samir Abed	DEPARTMENT Information Systems Architecture		DEPARTMENT NUMBER 5500
OWNER APPROVAL		DATE	EXTENSION 71248
PAS CORE TEAM APPROVAL DATE		CIO APPROVAL DATE	SIGNATURE
TECHNICAL TEAM Information Security		NEXT REVIEW DATE → February 1, 2005	

### I. PURPOSE

This policy is designed to ensure protection of Amgen Information System user-based authentication mechanisms and to prohibit sharing of accounts.

Authentication assures user identities are validated and authorization assures authenticated individuals are granted appropriate levels of system access and transaction capabilities.

Passwords, private key credentials, and tokens are specifically designed to identify and authenticate users to Amgen systems and maintain confidentiality of Amgen business-related information by providing access only to legitimate users. Because system and network access is granted based on those authentication mechanisms, all user ID/passwords and other advanced authentication mechanisms must be protected from disclosure.

### II. SCOPE

This policy applies to all Amgen full-time and part-time staff worldwide, as well as temporary workers, contractors and consultants, and other individuals or companies that have access to the Amgen Network.

### III. POLICY

All identifications, passwords, tokens, telephone numbers, and other "access mechanism" to computing resources are proprietary and confidential to Amgen. All "access mechanisms" that are used in connection with Amgen's Information Systems shall not be revealed by the owner of the "access mechanism" to any other person or entity. Passwords shall be changed with consideration to the level of access that they provide and the frequency of their usage.

1. Each holder of an "access mechanism" is responsible for the safeguarding of "access mechanisms" provided to him/her. Holders of such "access mechanisms" are accountable for the unauthorized or negligent disclosure.
2. All individuals may access, or attempt to access, only data or other computing resources, which he/she is authorized to access as part of one's business roles and responsibilities.

3. Use of a public key based encryption system is permitted only with first providing Amgen the ability to decrypt any encrypted data.
4. Passwords shall only be stored in a manner that ensures that they cannot be compromised. Adequate protection shall be provided against unauthorized access.
  - a. When access codes / mechanisms are physically stored they shall be kept in an access controlled space.
  - b. Passwords shall always be encrypted when stored or transmitted.
  - c. Automated processes that require passwords must be protected from unauthorized disclosure

Instructions on how to change your password can be found at [www.amgen.com/password](http://www.amgen.com/password).

#### IV. EXCEPTIONS OR WAIVER REQUIREMENTS

Requests for exceptions to this policy shall be submitted to the chairman of the IS Policies and Standards Council on the approved waiver template. The waiver request shall be processed according to the documented waiver process.

#### V. COMPLIANCE

Continuous logging and auditing of network logons shall be used to measure compliance.

It is the responsibility of every employee to report any suspected or confirmed violations of this policy to his or her manager.

#### VI. GLOSSARY

**Access mechanism:** Any token, password, pin, certificate, or biometric data used to authenticate.

**Token:** A device provided to a user to provide additional authentication assurance. Ie: SecureID token

**Private key:** The private side of a public key based system that represents the user/entity.

#### VII. REFERENCES

N/A

#### VIII. DOCUMENT HISTORY

NUMBER	DESCRIPTION OF CHANGE	INITIATOR	ISSUE DATE
POL-021-000	Initial Version	Dave Ellison	10/22/01
POL-021-001	Revised	Dave Ellison	03/15/02
POL-021-002	Updated / Revised more information Split into policy and standard	J. Callahan	March 15, 2004