

<b>AMGEN®</b>	<b>POLICY</b>		
TITLE <b>INFORMATION SYSTEMS SECURITY POLICY</b>	CONTROL NUMBER <b>POL- 110-000</b>	EFFECTIVE DATE <b>25 June 2003</b>	

## *Amgen Information Systems Security Policy*

### **Background**

We rely heavily on our information systems to conduct business. As we evolve into the best human therapeutics company and our dependence on information systems increases, it is critical that Amgen staff understand their responsibilities regarding information and systems protection.

### **Purpose**

This policy document will provide the framework from which information security at Amgen will be governed.

### **Applicability**

This policy applies to all Amgen full-time and part-time staff worldwide, as well as temporary workers, contractors and consultants, to the extent permitted by applicable laws.

### **Policy**

#### **I. Organizational Security**

##### **1. Management of Information Security**

Amgen's Chief Information Officer is responsible for providing a secure information systems environment. To that end, the CIO will appoint an Information Systems Security Officer (ISSO) to act as his/her representative for all matters related to IS Security. In turn the ISSO will be responsible for the management and oversight of all IS security related activities.

##### **2. Allocation of Information Systems (IS) Security Responsibilities**

Every Amgen staff member is responsible for information security. Each Amgen information system must have an appointed custodian for that system or service. System/service custodians are responsible for ensuring compliance with all Amgen policies, standards and procedures.

##### **3. Security Awareness Training**

All Amgen staff members must be provided training regarding the appropriate use of Amgen systems. This training should also include the responsibilities of staff members for protecting Amgen's systems.

<b>AMGEN®</b>	<b>POLICY</b>	
TITLE <b>INFORMATION SYSTEMS SECURITY POLICY</b>	CONTROL NUMBER <b>POL- 110-000</b>	EFFECTIVE DATE <b>25 June 2003</b>

## **II. User Responsibilities**

### **1. User Authentication Responsibility**

Users must select strong passwords that are resistant to common attacks. Users are responsible for all activity that takes place within the context of their login. Users provided with authentication devices such as passwords and or tokens, to Amgen systems, are responsible for safeguarding these devices.

### **2. Unattended Computer Equipment**

Unattended computers must be secured. Users are required to log off prior to leaving a system physically unattended or electronically lock the system to prevent unauthorized use of the system.

### **3. Incident Reporting**

Incidents can include, but are not limited to, unauthorized access, the presence of malicious software, network intrusions, and denial of service attacks. Any individual detecting an incident or a violation of IS Security policy, or who observes questionable activity involving Amgen's computer systems must report the incident to the I.S. Security Department's hotline, at x79672.

## **III. Infrastructure Protection**

### **1. Network Access Controls**

Access to resources on the Amgen network will be controlled to prevent unauthorized use. A minimum of two-factor authentication is required to access any Amgen system. Network perimeter devices must have adequate controls to ensure no loss of confidentiality, integrity or availability. The connection of non-Amgen systems to the Amgen network is prohibited. This includes all types of devices such as laptops, workstations and PDA's.

### **2. User Access Management**

All systems must be configured in a manner to allow access only to authorized individuals.

### **3. Application Access Controls**

All applications must be configured in a manner to allow access only to authorized individuals.

TITLE	CONTROL NUMBER	EFFECTIVE DATE
INFORMATION SYSTEMS SECURITY POLICY	POL- 110-000	25 June 2003

**4. Software for Protecting Systems**

All systems are required to contain software to prevent the infection and/or spread of malicious software.

**5. Publicly Available Systems**

Information systems that are accessible by the general public must be hardened and protected to resist attack. In addition these systems must be controlled and segregated in such a way as to not increase the risk level of other systems.

**6. Third Party Access to Amgen**

Access to Amgen information systems by third parties will only be permitted following a detailed review of the requirements, risks and business value.

**7. Inventory of Information Assets**

An inventory of all IS assets, both hardware and software, will be maintained. This inventory must indicate the staff member accountable for the asset.

**8. Incident Management Procedures**

A Security Incident Response Team (SIRT) will be maintained to respond to IS security incidents.

**IV. Physical Security****1. Secure Areas**

Physical access to rooms that contain Amgen IS assets will only be granted on a need to have basis. Physical security procedures will be established to protect areas designated for limited access.

**2. Equipment Protection**

Amgen furnished computer equipment must employ at least one physical control to protect the system from theft. Additional or more stringent controls should be applied commensurate with the value of the equipment and the value of the information it might contain.

**V. System Life Cycle Management****1. System Development**

When developing new systems, appropriate security measures must be applied throughout the process. These measures must consider the business value of the

<b>AMGEN<sup>®</sup></b>		<b>POLICY</b>	
TITLE <b>INFORMATION SYSTEMS SECURITY POLICY</b>		CONTROL NUMBER <b>POL- 000-000/</b>	EFFECTIVE DATE <b>24 June 2003</b>

information, the potential business damage resulting from a failure in availability, confidentiality and/or data integrity and the likelihood of such an occurrence.

## 2. Disposal of IS Assets or Media

All IS assets or electronic media that are to be disposed must be free of any Amgen information prior to disposal. Disposal of any IS asset or media must be done via authorized disposal procedures to ensure adequate destruction.

## 3. Re-use of Systems

Prior to re-using Amgen information systems, all information contained within the system must be removed.

# VI. Disaster Backup and Recovery

## 1. Disaster Backup Plan

A disaster recovery plan must be established, maintained, and tested to ensure adequate measures have been taken to restore Amgen's information systems capabilities in the event of an emergency.


## 2. Information Backup

All information systems containing valuable data must be backed up on a regular basis in accordance with the value of the information.

# VII. Audit

## 1. Information System Logs

All information systems must keep accurate logs that provide the capability to analyze, recreate or synchronize events that have taken place.

  
Dr. Hassan Dayem

25 Jun 03  
Date