CSIRT Sample Policies

csirt.org/sample_policies/index.html

Sample Computer Usage Guidelines. This document establishes computer usage guidelines for the Systems Division support staff in the course of their job duties on Computer Systems. These guidelines incorporate the elements of the Systems Division Special Access Agreement and the Acceptable Use Statement of Systems Division Computing Resources. These guidelines are intended to protect the rights and privacy of Systems Division clients as well as those of Systems Division support staff. Any Corporate Headquarters guidelines or policies will take precedence over these guidelines.

Acceptable Use Statement. The following document outlines guidelines for use of the computing systems and facilities located at or operated by () The definition of Systems Division and computing facilities will include any computer, server or network provided or supported by the Systems Division

Special Access Policy. Special access on systems is maintained and monitored, via the Special Access database, by both Operations and the Security Officer and/or assistant.

Special Access Guidelines Agreement. This agreement outlines the many do's and do not's of using special access on NAS computers. Special access is defined as having the privilege and password to use one or more of the following accounts: () . The NAS environment is very complex and dynamic.

Network Connection Policy. This policy describes the requirements and constraints for attaching a computer to the work. All computers installed on the network fall under the authority and responsibility of the Data Processing Installation Computer Security Officer (DPICSO) and as such they must meet the minimum security requirements regulations and policies.

Escalation Procedures for Security Incidents. This procedure describes the steps which are to be taken for physical and computer security incidents which occur within the facility. The physical security incidents covered in this procedure are: theft (major and minor), illegal building access and property destruction (major or minor).

Incident Handling Procedure. This document provides some general guidelines and procedures for dealing with computer security incidents. The document is meant to provide support personnel with some guidelines on what to do if they discover a security incident.

Acceptable Encryption Policy. The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Analog/ISDN Line Security Policy. This document explains analog and ISDN line acceptable use and approval policies and procedures. This policy covers two distinct uses of analog/ISDN lines: lines that are to be connected for the sole purpose of fax sending and receiving, and lines that are to be connected to computers.

Guidelines on Anti-Virus Process. Recommended processes to prevent virus problems.

Application Service Providers (ASP) Policy. This document describes Information Security's requirements of Application Service Providers (ASPs) that engage with .

Acquisition Assessment Policy. To establish InfoSec responsibilities regarding corporate acquisitions, and define the minimum security requirements of an InfoSec acquisition assessment.

ASP Security Standards. This document defines the minimum security criteria that an Application Service Provider (ASP) must meet in order to be considered for use by .

Audit Policy. To provide the authority for members of 's InfoSec team to conduct a security audit on any system at

.

Automatically Forwarded Email Policy. To prevent the unauthorized or inadvertent disclosure of sensitive company information.

DB Password Policy. This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of 's networks.

Dial-In Access Policy. The purpose of this policy is to protect 's electronic information from being inadvertently compromised by authorized personnel using a dial-in connection.

DMZ Lab Security Policy. This policy establishes information security requirements for all networks and equipment deployed in labs located on the "De-Militarized Zone" (DMZ).

Extranet Policy. This document describes the policy under which third party organizations connect to networks for the purpose of transacting business related to .

Information Sensitivity Policy. The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of without proper authorization.

Internal Lab Security Policy. This policy establishes information security requirements for labs to ensure that confidential information and technologies are not compromised, and that production services and other interests are protected from lab activities.

Internet DMZ Equipment Policy. The purpose of this policy is to define standards to be met by all equipment owned and/or operated by located outside 's corporate Internet firewalls.

Lab Anti-Virus Policy. To establish requirements which must be met by all computers connected to lab networks to ensure effective virus detection and prevention.

Password Policy. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of 's entire corporate network. As such, all employees (including contractors and vendors with access to systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Remote Access Policy. The purpose of this policy is to define standards for connecting to 's network from any host. These standards are designed to minimize the potential exposure to from damages which may result from unauthorized use of resources.

Risk Assessment Policy. To empower InfoSec to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Router Security Policy. This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of .

Server Security Policy. The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by . Effective implementation of this policy will minimize unauthorized access to proprietary information and technology.

THIRD PARTY CONNECTION AGREEMENT. This Agreement is the complete agreement between the parties hereto concerning the subject matter of this Agreement and replaces any prior oral or written communications between the parties.

Virtual Private Network (VPN) Policy. The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the corporate network.

Wireless Communication Policy. This policy prohibits access to networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by InfoSec are approved for connectivity to 's networks.