XYZ Corporation

# IT/Cybersecurity Policies & Procedures

NIST 800-171 Compliance

<XYZ Corporation>
3-7-2016

## Mission Statement

*(Insert Company's mission statement here)*

## Introduction

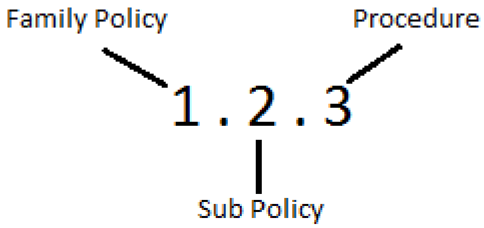
This Policies and Procedures Manual is a reference for employees of XYZ Corporation, pertains only to controlled unclassified information, and is intended to comply and cover all requirements described in NIST 800-171.

This manual does not and cannot describe all the policies and procedures employees are expected to observe and follow.  However, the Manual and the Employee Guidelines supersede all prior policy and procedure guidelines as well as all statements or commitments, oral or written, concerning the policies employees are expected to observe or the procedures employees are expected to follow while employed with the Company.  The Company reserves the right, whether in an individual situation or more generally, to interpret, supplement, replace, suspend, vary, change, or eliminate any of the policies and procedures and to adopt new ones at any time, with or without notice.  If an employee has a questions or concerns regarding a Company policy or the procedures he or she is to follow, the employee is responsible for contacting his or her supervisor, manager, Human Resource Representative, or the President for clarification.

## Responsibility & Authority Matrix

| Role | Person(s) Appointed | Responsibilities & Authority |
|---|---|---|
| CM – Corporate Management | CEO/President & Department VP's | Responsible for the company mission, security, and reputation.  Appoints and oversees all other roles. |
| CCB – Change Control Board | Appointed section leads | Reviews/approves changes to policies, procedures, configurations, maintain documentation, etc. |
| SO – Security Officer | FSO/ISSM | Coordinates key physical and personnel security functions. |
| ITA – Information Technology Authority | CIO, IT Director, or appointed individual | Executive authority over the company's Information technology. |
| ITM – Information Technology Manager | ITD Manager | Ensures day to day execution of policies, procedures, and practices are carried out by the ITD. |
| DM – Department Manager | Program Manager, HR Manager, Line Manager, etc. | Manager of a specified area of the company. |

## Explanation of Policy Numbering



# Contents

| Current Revision # | 1.0 | CCB Approval Date | 20160218 |
|---|---|---|---|

# 1.0.0 Access Control Policy

It is the policy of XYZ Corporation to manage all Information and Communication Technology (ICT) assets on the XYZ Corporation network in accordance with best practices for both efficiency and security; and to maintain compliance with contractual obligations, certification requirements, and applicable laws.

### Purpose

It is the purpose of this section to outline the policies and procedures for access control.  Any exceptions to these procedures must be approved by CM and Human Resources and documented to any extent necessary to prove due diligence in the event of an audit or incident.

This section includes policies and procedures on the following subjects:

### Scope

This policy applies to all XYZ Corporation employees, contractors, vendors and agents with a company-owned or personally-owned computer, workstation, mobile, or electronic device used to connect to the XYZ Corporation network.

## 1.1.0 Account/System Management Policy

It is the policy of XYZ Corporation to manage the admission to system and network resources so that approved individuals will be granted access to only that required to perform their duties and no more. XYZ Corporation will also provide and maintain electronic data for the corporation and its subsidiaries in a manner that meets high standards for availability, integrity, and accountability.

Referenced NIST 800-171 Requirements

3.1.1; 3.1.2; 3.1.3; 3.1.4; 3.1.5; 3.1.6; 3.1.7; 3.1.8; 3.1.9; 3.1.10; 3.1.11; 3.1.16; 3.1.17; 3.1.21; 3.1.22

Referenced NIST 800-53 Controls

AC-02-00; AC-03-00; AC-04-00; AC-05-00; AC-06-00; AC-06-01; AC-06-02; AC-06-05; AC-06-09; AC-06-10; AC-07-00; AC-08-00; AC-11-00; AC-11-01; AC-12-00; AC-18-00; AC-18-01; AC-20-02; AC-22-00

### 1.1.1 Account Creation Procedure

All account creations will be submitted by the requesting DM to the ITD for completion using the Account Request Ticketing System. All required fields must be completed before the account can be created. If a non-standard account is needed, the request will be submitted to the ITA for review. The ITA will determine if the request will be approved/denied and submitted to the ITD for creation or if it will need to be reviewed/approved by the CCB.

The following relates to standard accounts:

- DM will be responsible for stating start and end dates of access for each system account. End dates will be set on accounts within Active Directory if applicable.
- Systems administrators and members of the ITD shall respond and act accordingly to requests within a timely fashion, offering at least a 24-hour turnaround for account creation.
- During such tenure, the temporary account holder shall do work when accessing, using, or relying on XYZ Corporation infrastructure within the bounds of all policies and procedures. Any policies or procedures listed and cited within the Facilities Security Plan (FSP) of XYZ Corporation or its subsidiaries shall be considered governing above and beyond this procedure.
- Should a definite end date and time apply to any employee, contractor, or other account holder, the ITD shall create the account with the proper disablement times as stated by the DM.

Supplemental Information

XYZ Corporation defines the types of information system accounts to support organizational missions/business functions such as:

- Standard
  - Full Time Employee
  - Part Time Employee
  - Temporary Account
  - Contractor
  - Consultant

- Non-Standard
  - Administrative Account
  - System/Application Account
  - Specialized Account

Forms

N/A

### 1.1.2 Assign Network Access Procedure

To maintain the accountability and integrity of XYZ Corporation information systems, it is best practice to maintain account rights and permissions in a method of "most restrictive" meaning that account permissions shall be configured to provide the user access to only those resources required, and no excessive permissions shall be granted.

User roles will be established based on type of work performed, as well as contracts, proposals, and projects that require specific XYZ Corporation information systems resources. Each role defined and its required rights will be documented and audited to ensure proper availability, accountability, and integrity of the role.

XYZ Corporation information systems resources shall be assigned in groups based on role access, and user accounts will be added or removed from these groups based on role classification as required. Each resource may be assigned multiple groups with varying levels of rights based on such roles to allow for "most restrictive" access to those that may not need elevated rights.

In the event of a role or account change, the DM requesting the change must submit an Account Modification ticket to the ITD. The ITD will then notify the ITA which will review and supply an approval or denial of request. If approved, the ITD will complete the request in a timely manner. Quarterly audits of all user access and roles will be performed to ensure proper access and procedural controls.

Forms

N/A

### 1.1.3 Privileged Accounts/Functions Procedure

If elevated privileges are required/desired, such rig
account with elevated rights may be created to r
actions as it pertains to XYZ Corporation info
create a second user account with el
However, in some cases t

All reques
the D