Information Technology Security Plan
Policies, Controls, and Procedures
Identify Governance ID.GV

Location:

<table>
<thead>
<tr>
<th>ID.GV Governance</th>
</tr>
</thead>
</table>
| **ID.GV-1**  
Establish Information Security Policy |
| **ID.GV-2**  
Coordinate and Align Information Security Roles and Responsibilities with Internal Roles and External Partners |
| **ID.GV-3**  
Understand & Manage Legal & Regulatory Cybersecurity Requirements |
| **ID.GV-4**  
Governance and Risk Management Processes Address Cybersecurity Risks |
# Information Security Policy and Procedures

## Identify Governance ID.GV

### Table of Contents

<table>
<thead>
<tr>
<th>Item</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify Governance (ID.GV) Overview</td>
<td>3</td>
</tr>
<tr>
<td>Establish Information Security Policy (ID.GV-1)</td>
<td>4</td>
</tr>
<tr>
<td>- Risk Management:</td>
<td>4</td>
</tr>
<tr>
<td>- Compliance Management:</td>
<td>6</td>
</tr>
<tr>
<td>- Resources Required</td>
<td>6</td>
</tr>
<tr>
<td>- Links to Supporting Policies, Documentation, and Resources</td>
<td>6</td>
</tr>
<tr>
<td>Coordinate and Align Information Security Roles and Responsibilities with Internal Roles and External Partners (ID.GV-2)</td>
<td>7</td>
</tr>
<tr>
<td>- Risk Management:</td>
<td>8</td>
</tr>
<tr>
<td>- Compliance Management:</td>
<td>11</td>
</tr>
<tr>
<td>- Resources Required</td>
<td>11</td>
</tr>
<tr>
<td>- Links to Supporting Policies, Documentation, and Resources</td>
<td>11</td>
</tr>
<tr>
<td>Understand and Manage Regulatory Cybersecurity Requirements ID.GV-3</td>
<td>12</td>
</tr>
<tr>
<td>- Risk Management:</td>
<td>12</td>
</tr>
<tr>
<td>- Compliance Management:</td>
<td>12</td>
</tr>
<tr>
<td>- Resources Required</td>
<td>12</td>
</tr>
<tr>
<td>- Links to Supporting Policies, Documentation, and Resources</td>
<td>12</td>
</tr>
<tr>
<td>Governance and Risk Management Processes Address Cybersecurity Risks ID.GV-4</td>
<td>12</td>
</tr>
<tr>
<td>- Risk Management:</td>
<td>14</td>
</tr>
<tr>
<td>- Compliance Management:</td>
<td>14</td>
</tr>
</tbody>
</table>
Resources Required......................................................................................14
Links to Supporting Policies, Documentation, and Resources........14
Identify Governance (ID.GV) Overview

The policies, procedures, and processes to manage and monitor NDCBF’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the elder board and leadership of cybersecurity risk.

Identify Governance functions are:

- **Establish Information Security Policy ID.GV-1** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
  - **ID.GV-1 will contain all NDCBF IT security policies**

- **Coordinate and Align Information Security Roles and Responsibilities with Internal Roles and External Partners ID.GV-2** – NDCBF’s information security roles & responsibilities are being defined, coordinated, and aligned with internal leadership and staff and external partners.

- **Understand and Manage and Regulatory Cybersecurity Requirements ID.GV-3** - Legal and regulatory requirements regarding NDCBF’s cybersecurity, including privacy and civil liberties obligations, are researched, defined, understood and managed. This section will include overall definitions for PCI DSS, HIPAA and Texas House Bill 300, and overall risk management.

- **Governance and Risk Management Processes Address Cybersecurity Risks ID.GV-4** – NDCBF’s governance and risk management processes are being developed to address cybersecurity risks.
Establish Information Security Policy (ID.GV-1)

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform management of cybersecurity risk.

Primary Control Reference - NIST SP 800-53 Rev. 4-1 Controls from all families

NDCBF IT Security Policies - Defined by the security committee

- 5K Technical Services maintain inventory of all information systems and other systems that touch the network
- 5K Technical Services monitor all information systems and other systems that touch the network
- All mobile devices are to be encrypted
- Access to the private and public network
- All NDCBF work is to be done on NDCBF owned computer devices – There is an outstanding issue on the use of personal mobile phones used for NDCBF work - email

Risk Management:

- eRisk Self-Assessment 1) Security Policy
  - 1.1) Does your company have a current enterprise-wide computer network and information security policy that applies to all employees, independent contractors and third-party vendors?
    - Best practice: A formal policy informing employees and contractors of their obligation to perform information security tasks as part of their ongoing job duties is essential. It should be drafted and implemented through senior management and the IT security function.
  - Answer: Work in progress
  - 1.2) Has the enterprise-wide computer network and information security policy been approved by the Board of Directors (when
required by industry regulation such as GLBA) and/or by executive management?
  ▪ Best practice: The information security policy must carry the weight of approval by organizational authority if it is to be implanted and enforced in an effective manner.
  ▪ Answer: Work in progress

1.3) Describe how employees and/or customers using your network formally acknowledge their agreement to adhere to the terms of your policy (e.g., signed employment forms, orientation training, computer-based training sessions and quizzes with mandated “pass rates”, click-assent to Terms and Conditions on retail Internet sites, etc.)?
  ▪ Example Answer: Signed employee handbook receipt form. PCI training delivered via LMS for those employees with credit/debit card involvement.

1.4) Does the information security policy specify "Acceptable Use" of all company-owned computer/network resources, including proper use of e-mail and access to the Internet (and highlighting mandatory prohibitions against the following: visiting adult sites, exporting of company-proprietary information, illegal downloading of copyright-protected content such as MP3 music files, or illicit posting of company-confidential material in publicly-accessible message boards or chat rooms)?
  ▪ Best practice: In most cases, violations of the security policy are unenforceable without clearly defined 'acceptable use' guidelines, notices, and instructions.
  ▪ Answer: Work in progress

1.5) Does the information security policy have a named owner who is responsible for review and periodic proposal of updates to executive management?
  ▪ Best practice: A security policy without a manager responsible for implementation is of limited value. Information security is rarely viewed as a priority outside the IT organization.
Answer: Work in progress
- 1.6) Have you published the information security policy within the company (via the corporate Intranet, employee handbooks, etc.)?
  - Best practice: If information security policies are not publicized, the company cannot reasonably expect uniform adherence to them by every employee. Even well-meaning employees may not be aware of the technology-based requirements that may be included in the company's procedures. Moreover, this may help to meet any legal requirements about notice and assent.
- Answer: Work in progress
- 1.7) Is your policy supported through a well-developed set of approved standards, guidelines, and procedures that are designed to facilitate compliance with the policy?
- Answer: Work in progress

COMPLIANCE MANAGEMENT:
- PCI Compliance Requirements
  - 12.1 Establish, publish, maintain, and disseminate a security policy. Is a security policy established, published, maintained, and disseminated to all relevant personnel?
  - 12.1.1 Review the security policy at least annually and update the policy when the environment changes.
- HIPAA AND TEXAS HOUSE BILL 300
  - Requirements and questions that apply

RESOURCES REQUIRED
Support agreements and other resources required to execute

LINKS TO SUPPORTING POLICIES, DOCUMENTATION, AND RESOURCES
- Document
- Document
- Document
Coordinate and Align Information Security Roles and Responsibilities with Internal Roles and External Partners (ID.GV-2)

NDCBF’s information security roles & responsibilities are being defined, coordinated, and aligned with internal roles and external partners.

Primary Control Reference - NIST SP 800-53 Rev. 4 PM-1, PS-7

- PM-1 INFORMATION SECURITY PROGRAM PLAN - Control:
  The organization:
  - Develops and disseminates an organization-wide information security program plan that:
    - Provides an overview of the requirements for the security program and a description of the security management controls in place or planned for meeting those requirements;
    - Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
    - Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
    - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations;
  - Reviews the organization-wide information security program plan [Assignment: organization defined frequency];
  - Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
  - Protects the information security program plan from unauthorized disclosure and modification.
• **PS-7 THIRD-PARTY PERSONNEL SECURITY** – Control: The organization:
  o Establishes personnel security requirements including security roles and responsibilities for third-party providers;
  o Requires third-party providers to comply with personnel security policies and procedures established by the organization;
  o Documents personnel security requirements;
  o Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and
  o Monitors provider compliance.

• An inventory of external third-party providers is maintained in **ID-AM-6 Establish Roles and Responsibilities for Workforce and 3\textsuperscript{rd} Party Stakeholders**

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21

**Risk Management:**

• eRisk Self-Assessment 2) Security Organization
  o 2.1) Is there a senior company manager who is directly charged with responsibility for enterprise-wide information security strategy and operational compliance?
Best practice: From an audit and accountability perspective, it is essential that one individual is identified as 'owning' the information security function within a company.

Sample Answer: Yes - But With Other Duties As Well

2.2) Is there a departmental function within the company that is staffed with dedicated or non-dedicated information security employees who assist the information security manager in carrying out compliance operations?

Best practice: This may or may not be applicable depending on the size of your company. Companies with significant assets and/or complex network operations usually need a dedicated team to properly maintain a secure network environment. Moreover, security functions can overwhelm a CIO or IT manager who is primarily concerned with maintaining network operations.

Sample Answer: Partial - Security Tasks Assigned Among IT Employees

2.3) Describe the IT security department in terms of staffing, specializations, current certifications, budget, and defined roles/responsibilities of individual members.

Answer: Certain staff members share responsibility for security tasks that are not very technical on an as-needed basis. Technical security tasks are outsourced to 5K Technical Services. This includes daily reviews of firewall and IDS/IPS systems for possible attacks.

2.4) Does the company perform routine audits (or have them performed by an external vendor) of all activities from an information security perspective?

Best practice: The information security officer should perform regularly scheduled audits to ensure that employees and contractors are complying with the formal information security policy. This may be as simple as a written test or onsite spot checks.
• Work in progress
  
  o 2.5) Please describe the existing schedule for both internal and external IT security audits. Also, identify the completion date of the most recent audit and who performed it. Please include any references to a SAS 70, and whether the most recent audit found significant weaknesses or areas for improvement, and whether these have been implemented.

  • Regular security audits are not done at this time
  
  o 2.6) If the company maintains dedicated network connectivity with - or outsources mission-critical IT functions to - third-party clients/vendors, are there adequate contractual provisions and sufficient functional controls in place to enforce your information security policy and procedures?

  • Best practice: Without legally enforceable security language in outsourcing contracts (SLAs), the company has little recourse in the event of a network security breach caused by negligence on the part of a vendor. Many vendors view network security protection as a 'service feature' that must be purchased separately from the primary business service.

  • Work in progress

  o 2.7) Please describe how you assess the risks associated with your vendors' IT security controls and practices as part of a defined vendor management program. Identify a few of the key clients/vendors whom you have assessed as part of this program during the past year.

    • Sample Answer: We ask them to complete a security questionnaire and then negotiate on possible gap items.

  o 2.8) Are Computer Emergency Response Team and vendor advisories related to security problems monitored and applied as soon as possible to all affected systems (i.e. software vulnerability patches, antivirus updates, etc.)?
• Best practice: Installing patches and updates on a regular basis is a critical network security function, especially in Unix and Microsoft environments.

  o 2.9) Please identify which tools you use to deploy system patches within your environment (examples might include Microsoft's WSUS or SCCM, or other third party vendor offerings).

  ▪ Work in progress

**COMPLIANCE MANAGEMENT:**

• PCI Compliance Requirements
  o Requirements that apply

• HIPAA AND TEXAS HOUSE BILL 300 Requirements
  o Requirements and questions that apply

**RESOURCES REQUIRED**

• Support agreements and other resources required to execute

**LINKS TO SUPPORTING POLICIES, DOCUMENTATION, AND RESOURCES**

• Document
• Document
• Document
Understand and Manage and Regulatory Cybersecurity Requirements ID.GV-3

Legal and regulatory requirements regarding NDCBF’s cybersecurity, including privacy and civil liberties obligations, are researched, defined, understood and managed.

Primary Control Reference - NIST SP 800-53 Rev. 4 4 -1 controls from all families (except PM-1)

**Risk Management:**
- eRisk Self-Assessment
  - Questions that apply

**Compliance Management:**
- PCI Compliance Requirements
  - Requirements that apply
- HIPAA AND TEXAS HOUSE BILL 300 Requirements
  - Requirements and questions that apply

**Resources Required**
- Support agreements and other resources required to execute

**Links to Supporting Policies, Documentation, and Resources**
- Document
- Document
- Document

Governance and Risk Management Processes Address Cybersecurity Risks ID.GV-4

NDCBF’s governance and risk management processes are being developed to address cybersecurity risks.

Primary Control Reference - NIST SP 800-53 Rev. 4 PM-9, PM-11
• **PM-9 RISK MANAGEMENT STRATEGY** - Control: The organization:
  o Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
  o Implements the risk management strategy consistently across the organization; and
  o Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.

  Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization’s risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive. Related control: RA-3. Control Enhancements: None.


• **PM-11- MISSION/BUSINESS PROCESS DEFINITION** - Control: The organization:
  o Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and
  o Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

  Supplemental Guidance: Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an
organization’s information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.
Control Enhancements: None.
References: FIPS Publication 199; NIST Special Publication 800-60

**RISK MANAGEMENT:**

- eRisk Self-Assessment
  - Questions that apply

**COMPLIANCE MANAGEMENT:**

- PCI Compliance Requirements
  - Requirements that apply
- HIPAA AND TEXAS HOUSE BILL 300 Requirements
  - Requirements and questions that apply

**RESOURCES REQUIRED**

- Support agreements and other resources required to execute

**LINKS TO SUPPORTING POLICIES, DOCUMENTATION, AND RESOURCES**

- Document
- Document
- Document