Toolkit

The Vendor-Free IT Community.

IT GOVERNANCE & COMPLIANCE

These NOREX Member-contributed documents include topics such as confidentiality, data classification, plans, policies & charters, PCI, privacy, records management, risk assessment, and staffing. | TK015

The NOREX Document Library is continually updated for the benefit of our Members. Please consider contributing documents from your organization. Thank you!

Confidentiality

DIGITAL INFORMATION TRANSMISSION. This policy details the standard approach to sending either public, confidential, or sealed digital information. 5 Pages (20-605)

ENCRYPTION STANDARD. This policy provides guidance and establishes a baseline for the use of encryption algorithms to protect information resources that contain, process, or transmit confidential and/or sensitive information (PII, PHI, PCI, etc.). 2 Pages (20-602)

PROVIDER CONFIDENTIALITY & SECURITY AGREEMENT. This agreement applies to any provider party who is on site or who requires access to the company network. 2 Pages (20-539)

GOVERNING SYSTEMS ACCESS. This policy provides a plan for the oversight of access to company information systems, media, hardware/software, Internet, and network systems. 3 Pages (20-288)

CONTRACTOR DATA INTEGRITY / CONFIDENTIALITY. This is an agreement template between an organization and services contractor. 1 Page (20-087)

DATA SHARING AGREEMENT. The following data sharing agreement template is HIPAA compliant. 3 Pages (20-086)

CONFIDENTIALITY AGREEMENT. This agreement template outlines the intent of both parties in regard to the protection of information. 2 Pages (20-084)

ACCEPTABLE USE / CONFIDENTIALITY. This agreement describes the standard policy of the use of company Information Technology resources and data contained therein. 5 Pages (20-043)

Data Classification

IDENTITY PROTECTION POLICY. This document provides regulations about Personal Identifying Information (PII), including what may be shared and what must remain confidential. 7 Pages (20-647)

DATA CLASSIFICATION & PROTECTION STANDARDS. This matrix lists several types of records, what they consist of, and how they must be handled, listing classifications of Sensitive, Confidential, Privileged, and Vital. 26 Pages (20-594)

INFORMATION CLASSIFICATION POLICY. Here is a system for classifying information resources according to the risks associated with storage, processing, transmission, and destruction. 5 Pages (20-531)

DATA CLASSIFICATION WORKSHEET. Information class, type, systems, availability, integrity, and confidentiality level are examples of these data classification tools. 4 Pages (20-530)

SECURITY CONTRACT LANGUAGE. The following document describes language frequently used in the development of security contracts. Topics include encryption, authentication, compliance, auditing, personal data, and requirements. 4 Pages (20-508)

DATA CLASSIFICATION PROJECT. This project ensures conformance with the information resources management program and that information resources are adequately protected. It also identifies the business owner responsible for the identification and classification of information. 13 Pages (20-454)

DATA CLASSIFICATION POLICY. This state policy provides a data classification methodology to state agencies for understanding and managing the confidentiality & criticality level of data & information systems. 9 Pages (20-453)

INFORMATION SECURITY CLASSIFICATION. Information at the company will be appropriately protected based on its value, confidentiality, sensitivity, and the risk of loss or compromise. This document helps with information classification. 7 Pages (20-158)

Discussions

PROJECT MANAGEMENT / PMO TRANSCRIPT. NOREX Members discussed the value a PMO returns to the business, the value of a PMO in a functional environment, introducing a PMO to an organization that is historically managed in silos, measuring success of a PMO for Agile Projects, the pros and cons of Waterfall vs. Agile, assigning projects, work intake process for smaller projects, tools to keep track of the lifecycle, documentation requirements for SDLC, the number of teams for ScrumMasters, and practicing Kanban. 23 Pages (NV2391)

VENDOR MANAGEMENT TRANSCRIPT. NOREX Members discussed flexible pricing strategies, holding vendors accountable for service delivery, strategies for maintenance / support agreements, handling vendors and items to document, implementing an IT VMO, tools for vendor management and vendor scoring, and assessing the maturity of your VMO and strategic vendor relationships. 17 Pages (NV2390)

SD-WAN TRANSCRIPT. NOREX Members discussed drivers to SD-WAN, reliability of their solution, negative experiences when implementing SD-WAN, recommendations for design and deployment, solutions evaluated for SD-WAN, utilizing providers with their own backbone vs. providers like CATO and Velo, access to all internet / Cloud services routed through NGFWaaS, and use of a managed service provider for SD-WAN. 22 Pages (NV2389)

FOOD & BEVERAGE MANUFACTURING: IT SECURITY TRANSCRIPT. NOREX Members discussed recommended IT Security initiatives, cybersecurity insurance and renewals, segregation of the IT network, communication to the outside world from the OT network, solutions used for 2FA on VPN connections, Artic Wolf, Red Canary, and documented recovery and response plans. 15 Pages (NV2386)

POST-COVID HYBRID WORK STRATEGIES TRANSCRIPT. NOREX Members discussed how best to manage a hybrid work environment, provisions for home offices, hardware support and budget, internet connectivity issues, cash allowances and potential legal concerns, achieving equity amongst in-office and at-home staff, best tools for building out conference rooms, and security. 30 Pages (NV2385)

POWER BI TRANSCRIPT. NOREX Members discussed getting started with Power BI, experiences with building and executing, visualization services, mining capabilities, dashboard viewing, licensing agreements, backup and recovery strategies, deliverables, and alternative products. 15 Pages (NV2383)

RANSOMWARE TRANSCRIPT. NOREX Members discussed Ransomware attacks and what to do once infected, restoring LAN shares and rebuilding workstations, warnings against paying ransom, counter measures and mitigation, backups and patching, cybercriminal activity detection, MDR vs. MSSP, endpoint protection, and the use of an MDM application. 30 Pages (NV2381)

CONSTRUCTION INDUSTRY: IT PROJECT MANAGEMENT TRANSCRIPT. NOREX Members discussed how best to elevate the presence of IT project management in the Construction Industry, community of practice standardization, master service integrators, Construction Management software, credential harvesting, and security. 14 Pages (NV2375)

SECURITY FRAMEWORKS TRANSCRIPT. NOREX Members discussed the hierarchy of security frameworks; most commonly used frameworks; categorization of control, platform, and risk frameworks; and active threat hunting. 14 Pages (NV2374)

GLOBAL IT ISSUES TRANSCRIPT. NOREX Members discussed the biggest issues they and their organizations are facing with a global footprint in today's business climate. The expectations with employees

able to return to the office, IT talent recruiting and hiring internationally, standardization of processes, cybersecurity, procuring equipment globally, keyboard sourcing, and in-country IT support were challenges shared by all Member participants. 17 Pages (NV2371)

MICROSOFT TEAMS BEST PRACTICES TRANSCRIPT. NOREX Members discussed the implementation of Microsoft Teams within an organization, Teams' members as part of the infrastructure or collaboration teams, the use of the exploratory license program, promoting adoption and usage of the platform, and VoIP integrations. 49 Pages (NV2369)

CLOUD-BASED STORAGE TRANSCRIPT. NOREX Members discussed the lessons learned, and difficulties experienced, when transitioning from on-prem storage to Cloud. The discussion covered the pros and cons of various Cloud platforms, security, policy and practices, and the dangers of accessibility. 17 Pages (NV2368)

IT SERVICE MANAGEMENT TRANSCRIPT. NOREX Members shared strategies and solutions in designing, creating, delivering, supporting, and managing IT Services within an organization. 22 Pages (NV2367)

DATA LOSS PREVENTION TRANSCRIPT. NOREX Members shared strategies, policies, and solutions to prevent sensitive or critical information from leaving the corporate network. 21 Pages (NV2366)

HYPERCONVERGED INFRASTRUCTURE TRANSCRIPT. NOREX members share experiences adopting a Hyperconverged Infrastructure including performance expectations, vendor options, and back-up strategies during this April 2021 WebForum. 16 Pages (NV2365)

INCIDENT & PROBLEM MANAGEMENT TRANSCRIPT. Member organizations discuss both incident and problem management best practices, tools, lessons learned, and more during this April, 2021 WebForum. Chat comments and polls are included. 24 Pages (NV2364)

IT CHANGE MANAGEMENT TRANSCRIPT. NOREX members discuss IT Change Management processes including recommended tools, governance approaches and communication protocols during this April 2021 session. 25 Pages (NV2363)

RISK MANAGEMENT TRANSCRIPT. NOREX members share strategies for identifying, managing and reporting risks during this February 2021 session. 21 Pages (NV2358)

SECURITY INITIATIVES FOR 2021 TRANSCRIPT. NOREX members share 2021 IT security plans including budgets, initiatives and tools during this January 2021 session. 34 Pages (NV2354)

IT GOVERNANCE TRANSCRIPT. Aligning IT with the business can be challenging work. In this discussion, members tackle strategies for implementing and getting buy in, working with the business to align goals, and the structures that have made Governance a more successful venture. 17 Pages (NV2353)

PLANNING FOR 2021 TRANSCRIPT. NOREX members share their expectations for IT budgets, staffing levels, security initiatives, user support trends and other 2021 issues during this December 2020 session. 19 Pages (NV2351)

MANAGING AND MONITORING REMOTE TEAMS TRANSCRIPT. NOREX Members share policies, procedures and tools for managing and monitoring remote workers during this August 2020 WebForum. 20 Pages (NV2339)

CYBERSECURITY TRANSCRIPT. NOREX Members share cybersecurity best practices and tool recommendations during this July 2020 WebForum. 19 Pages (NV2331)

PCI TRANSCRIPT. Members take a fresh look at all regulation, protection, and processes required to meet PCI data security standards (DSS) during this March, 2020 WebForum. 13 Pages (NV2314)

ISO 27001 AND SOC COMPLIANCE TRANSCRIPT. Small group discussion among 6 member companies to exchange information, solutions, and best practice around ISO 27001, SOC2, and other security-related compliance / certification. 18 Pages (NV2293)

VULNERABILITY MANAGEMENT TRANSCRIPT. NOREX members share recommendations on processes and tools to manage IT vulnerabilities and risks during this September 2019 WebForum. 20 Pages (NV2288)

DATA GOVERNANCE / GDPR / US PRIVACY LAWS TRANSCRIPT. NOREX members share recommendations on achieving compliance with various privacy regulations during this August 2019 WebForum. 25 Pages (NV2283)

MANAGING PRIVACY REGULATIONS TRANSCRIPT. NOREX members share strategies for complying with various privacy regulations such as GDPR and CCPA during this March 2019 WebForum. 15 Pages (NV2261)

IT GOVERNANCE TRANSCRIPT. NOREX members share recommendations for the establishment and management of an effective IT Governance practice during this January 2019 session. 11 Pages (NV2256)

GOVERNMENT: MS365 ADOPTION TRANSCRIPT. NOREX Members from Government agencies share strategies on the adoption of Microsoft's M365 licensing program during this October 2020 WebForum. 19 Pages (GSP100)

GOVERNMENT: REGULATORY COMPLIANCE TRANSCRIPT. NOREX Government members share their experiences with regulatory compliance during this June 2019 session. 10 Pages (GSP099)

CIO: ROLE / JOB DESCRIPTION OF THE CIO TRANSCRIPT. Senior IT leaders discuss the evolution of the Chief Information Officer role during this October 2020 session. 17 Pages (CV076)

CIO: IT'S ROLE IN BUSINESS SUCCESS TRANSCRIPT. Senior IT leaders share strategies for aligning IT with business objectives during this July 2020 WebForum. Topics include cloud computing, staffing, project prioritization and Business Intelligence tool recommendations. 20 Pages (CV075)

CIO: IT TRANSFORMATION TRANSCRIPT. This March 2019 session featured strategic-level discussion on starting the transformation process, gaining executive support, involving business units and developing roadmaps for cloud usage and mobile device management. 19 Pages (CV071)

GDPR

GDPR PLAN. This plan details EU General Data Protection Regulation procedures including business cards, right of access, data retention, and data processing. 3 Pages (20-459)

GDPR OVERVIEW. All the basic information describing the European General Data Protection Regulation (GDPR) is provided in this presentation. 12 Pages (50-277)

Governance Plans, Policies & Charters

IT GOVERNANCE POLICY. This policy establishes the process for prioritization, requirements definition, user participation, and rollout for development and implementation of major and minor projects. 4 Pages (20-1067)

eGOVERNMENT STRATEGY. This strategy template outlines the sustainable development of organizational capability and the implementation of technology. 11 Pages (20-987)

STRATEGIC PLAN OUTLINE. These slides provide a template for creating a strategic plan of initiatives for 2021 and beyond. 8 Pages (20-982)

IT GOVERNANCE GROUP. This presentation offers information on creating a governance framework promoting transparency, clarity, and consistency. 19 Pages (20-811)

DATA GOVERNANCE POLICY. This policy applies to all data, processes, and/or standards used within business units such as Human Resources, Sales, Operations, Purchasing, etc. (See also 20-707 & 20-709). 11 Pages (20-708)

GOVERNANCE PROJECT SCORE SHEET. A template for tracking and outlining the expected impact, performance results, compliance, and other aspects of a proposed project. 2 Pages (20-554)

GOVERNANCE INFORMATIONAL BRIEF. This template provides a format for creating your own executive leadership team governance brief. 2 Pages (20-552)

ADA COMPLIANCE & ACCOMMODATIONS. The Americans with Disabilities Act (ADA) provides equal access & protection for persons with disabilities. Policy detail for the workplace is provided here. 2 Pages (20-522)

INFORMATION GOVERNANCE CERTIFICATION REQUIREMENTS. The intent of this questionnaire is to assist procurement with the solicitation of vendor responses to the information governance policy. Elements included are HIPAA privacy, security, and records management compliance. 14 Pages (20-363)

TECHNOLOGY STEERING TEAM CHARTER. A partnership between Information Technology and business leadership, the Technology Steering Team (TST) represents a critical component of the overall technology governance process. 7 Pages (20-204)

SHAREPOINT GOVERNANCE GUIDE. A comprehensive governance plan can benefit information systems and the organizations it services. 95 Pages (20-117)

SHAREPOINT GOVERNANCE MODEL. The model is a comprehensive document identifying lines of ownership for business & technical teams, defining areas of responsibility and establishing appropriate usage of the SharePoint environments. 24 Pages (20-109)

SYSTEMS GOVERNANCE CHARTER. The Systems Governance Committee serves two roles, IT Governance and Project Portfolio Oversight. 4 Pages (20-083)

DATA GOVERNANCE PROGRAM CHARTER. This data governance structure provides requirements and guidelines for data management, processes, ownership, data types, classification and retention of data. 13 Pages (50-343)

DATA MANAGEMENT POLICY. This policy provides requirements and guidelines for data management, outlining the protection protocol necessary to ensure data remains safe and protected. 4 Pages (50-342)

ACTIVE DIRECTORY GOVERNANCE POLICY. This plan documents and governs the implementation of business rules & policies for the use of Active Directory, all interacting systems, roles, responsibilities, and methods of enforcement. 31 Pages (50-299)

DATA GOVERNANCE FRAMEWORK. This document describes how a sound data governance program includes a governing committee, a defined set of procedures, and a plan to execute those procedures. 4 Pages (50-289)

ENTERPRISE DATA GOVERNANCE. This journey into Enterprise Data Governance as seen by an experienced NOREX member gives insight into resources and directives. 9 Pages (50-249)

SOFTWARE GOVERNANCE BOARD. This document helps record the duties and members of the board charged with governance of software maintenance. 1 Page (50-222)

Gramm-Leach-Bliley Act

GRAMM-LEACH-BLILEY ACT SECURITY PROGRAM. This describes safeguards implemented to protect covered data and information in compliance with the FTC's Safeguards Rule of the Gramm-Leach-Bliley Act (GLBA). 4 Pages (20-764)

REPORT REQUIREMENTS SPECIFICATION TYPE 2. This template provides an overview of business needs, data sources, report filters, parameters, and formatting. 5 Pages (20-622)

PCI

MOBILE DEVICE MANAGEMENT POLICY. This policy establishes the specific standards, guidelines, and procedures to manage the issuance, operation, and security of mobile devices and services (both company-issued and BYOD), to access company computing resources. 19 Pages (20-378)

HOSPITALITY LOSS PREVENTION. This guide describes how the hospitality industry might handle loss prevention issues with hard keys, guest rooms, and guest property. 5 Pages (20-287)

AMENITY & SERVICES PAYMENT PROCEDURES. The hotel industry is linked to several others, such as gift shops, spas, and athletic clubs. The following are procedures for accepting payment for these types of services. 14 Pages (20-286)

HOSPITALITY PAYMENT PROCEDURES. In a hotel/motel industry, the following procedures are taken when accepting a credit card as payment. 6 Pages (20-285)

PCI SERVICE PROVIDERS. The roles and responsibilities related to service providers are outlined in this PCI compliance document. 6 Pages (20-284)

PCI ROLES & RESPONSIBILITIES. This document identifies and explains the roles and responsibilities for various Company positions in regard to PCI compliance. 10 Pages (20-283)

PCI REQUIREMENTS KEY. Payment Card Industry (PCI) requirements regarding security, development, and firewall/router configurations are outlined in this key. 19 Pages (20-281)

INCIDENT RESPONSE POLICY. This document outlines the credit card security incident response policy. 3 Pages (20-280)

CREDIT CARD SECURITY INCIDENT RESPONSE PLAN. The Incident Response Team, comprised of the Controller, the IT Manager, the Facilities Director, the Loss Prevention Supervisor, and the Senior Systems Administrator have established specific guidelines for safeguarding cardholder information. 12 Pages (20-279)

Privacy

PRIVACY POLICY. The following website privacy policy explains what information is collected, how it is used, and with whom it is shared. 7 Pages (20-954)

INFORMATION PRIVACY AND SECURITY REQUIREMENTS. Access to sensitive or regulated information is granted to third parties according to the following agreement. 7 Pages (20-739)

DATA PRIVACY POLICY. This Privacy Statement describes protection of personally identifiable information in conjunction with data privacy legislation. 6 Pages (20-460)

HIPAA PROTECTION CHEAT SHEET. This poster gives an at-a-glance reference for the protection and disposal of Protected Health Information (PHI). 1 Page (20-311)

Records Management

RECORDS RETENTION AND DISPOSITION. This policy is to ensure that all records, regardless of media, are managed throughout their entire lifecycle including final disposition. 7 Pages (20-749)

RECORDS MANAGEMENT STANDARD. This standard provides direction regarding the retention and destruction of records, as also explained in related documents 20-707 and 20-708. 27 Pages (20-709)

ELECTRONIC RECORDS RETENTION. This policy advances the best practices in capturing, managing, and retaining electronic records. 6 Pages (20-642)

RECORDS MANAGEMENT POLICY. This policy establishes the components and responsibilities of records management programs along with staff functions necessary to implement them. 2 Pages (20-640)

VITAL RECORDS PRICING. This document is an example of how to record cost & pricing for various vital records systems and filing. 1 Page (20-607)

RFP: RECORDS MANAGEMENT SYSTEM. This requests proposals for qualified contractors to provide a Records Management System to replace several existing systems. 217 Pages (20-164)

RFI: RECORDS MANAGEMENT SYSTEM. A department is seeking information from vendors that can provide an operationally proven web-based Commercial Off-The-Shelf (COTS) software law enforcement application framework to replace, among other functions, internally developed Records Management System. 32 Pages (20-163)

RECORDS MANAGEMENT POLICY. This document describes protection and preservation of records and security of confidential documents. 30 Pages (10-1697)

RECORD RETENTION. This provides an example of a record protection and retention schedule by function, and assigns levels of confidentiality. 20 Pages (10-1696)

Risk Assessment

VENDOR SECURITY QUESTIONNAIRE. Issues such as compliance, risk assessment, incident management, and requirements are itemized in this vendor survey. 3 Pages (20-887)

AUDIT CONTROLS POLICY. This policy defines the audit controls of the security management process for health information technology resources. 2 Pages (20-591)

RFI: INFORMATION SECURITY RISK ASSESSMENT. Requested here is a privacy and security risk assessment pursuant to the Health Insurance and Portability Accountability Act (HIPAA). 18 Pages (20-573)

VENDOR DATA & RISK ASSESSMENT. This worksheet provides data on vendors as well as a risk assessment & security questionnaire. 19 Pages (20-225)

SECURITY AUDIT QUESTIONNAIRE. Information Technology management, information security, and privacy are described in this questionnaire. 10 Pages (20-206)

SOFTWARE RISK ASSESSMENT SUMMARY. Using data from service overviews and assessments, a summary of software risk assessment is made, determining acceptable risk, concern, and red flags. 8 Pages (50-326)

THIRD-PARTY TECHNICAL RISK ASSESSMENT. This software service questionnaire for third-party providers covers technical assessment, IT governance & development, architecture, security, and support. 7 Pages (50-325)

SOFTWARE RISK ASSESSMENT INSTRUCTIONS. These instructions are for completing the technical risk assessment required for third-party product or service providers that host or maintain systems on behalf of the organization and have access to data. 2 Pages (50-324)

THIRD-PARTY RISK ASSESSMENT. This security questionnaire helps to diagnose possible risks with potential or current vendors. 2 Pages (50-314)

TECHNOLOGY RISK ASSESSMENT POLICY & PROCEDURE. Following is an overview of the technology risk management process steps and the associated roles and responsibilities. 3 Pages (50-290)

Staffing

CLINICAL INFORMATICS SPECIALIST. 4 Pages (20-394)

HIPAA BUSINESS ASSOCIATE AGREEMENT. This agreement template is between an organization and a HIPAA compliant organization. 7 Pages (20-085)

RECORDS MANAGER FOLLOWUP INTERVIEW. The following are appropriate questions for a second interview of a potential Records Manager. 5 Pages (20-021)

RECORDS & INFORMATION MANAGER SECOND INTERVIEW. Questions for a second interview of a prospective Records and Information Manager are below. 2 Pages (20-020)

RECORDS & INFORMATION MANAGER QUESTIONS. These questions are appropriate for the first interview of a potential Records and Information Manager. 6 Pages (20-019)

RECORDS SUPERVISOR 2ND INTERVIEW. These questions are designed for the second interview of a potential Records Supervisor. 1 Page (20-018)

RECORDS SUPERVISOR 1ST INTERVIEW. These questions are designed for the first interview of a potential Records Supervisor. 2 Pages (20-017)

GRC MANAGER. 2 Pages (50-298)