Toolkit

The Vendor-Free IT Community.

SECURITY

These NOREX Member-contributed documents include RFP, contracts, staffing, policies, procedures, plans, manuals, security charter, framework, security awareness, risk assessment, incident management, encryption, electronic signature, anti-virus & malware, cybersecurity, PCI, mobile computing, eDiscovery, vendor management, discussions, and polls. | TK002

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

This Toolkit contains documents that have been voluntarily contributed by NOREX Members with the full knowledge that other Members may use the documents in any manner they see fit. NOREX and its Members shall not be held liable for any statements or interpretations contained within the documents. This Toolkit and related documents may be used for NOREX promotional purposes. Unauthorized use or distribution to non-NOREX Members is strictly prohibited.

Anti-Virus, Malware, & Phishing

INFORMATION SECURITY AND THE FIRE TRUCK: MEMBER PERSPECTIVE. A NOREX Member provides his perspective on security teams and the reactive “fire truck” analogy. 2 Pages (50-354)

RANSOMWARE PREVENTION: MEMBER PERSPECTIVE. This document contains a NOREX Member’s perspective on the prevention of Ransomware attacks. 2 Pages (50-353)

PHISHING AWARENESS EMAIL & CERTIFICATE. This document includes templates for a certificate awarded to employees who report phishing scams and an email to send to their supervisors. 2 Pages (20-970)

SIMULATED PHISHING CAMPAIGNS. Given at the 2019 NOREX International Roundtable, this presentation delivers information on how and why a simulation of a phishing campaign can be valuable to your team. 16 Pages (20-695)

VIRUS PREVENTION POLICY. This policy is designed to ensure that IT resources and systems employ effective anti-virus and anti-malware detection software. 2 Pages (20-633)

PHISHING TEST POLICY. This policy describes the consequences of repeated failing of company phishing detection tests. 1 Page (20-590)

PHISHING E-MAIL POLICY. Forged or faked electronic documents and e-mail, referred to as phishing, can expose a user to financial or security risks. This document describes how to respond to phishing attacks. 1 Page (20-514)

PHISHING THREAT DASHBOARD. These charts document phishing threats using Websense and SCCM. 2 Pages (20-097)

SAFETY STEPS FOR ONLINE USERS. Practice these six simple steps for safety while online at work or at home. 1 Page (50-321)

UNWANTED/MALICIOUS E-MAIL PATH. These suggested steps are a guide for how unwanted and/or potentially malicious e-mail messages are identified and dealt with. 1 Page (50-193)

Cybersecurity

CYBER THREAT INTELLIGENCE. This overview of cyber threat intelligence, report writing tips, and intelligence-driven projects was presented at a NOREX event. 31 Pages (20-1088)

REMOTE WORK CYBERSECURITY GUIDELINES. This is a concise overview of cybersecurity guidelines in the COVID-19 era. 5 Pages (20-1074)

INFORMATION SECURITY METRICS DASHBOARD. Security metrics provide overall governance for the security program and operational metrics that create the foundation for measuring and reporting on important cybersecurity data points. 1 Page (20-1032)

LARGE CYBER INCIDENT HANDLING. This document provides technical best practices on handling large scale malware-related activity. 8 Pages (20-999)

SMALL CYBER INCIDENT HANDLING. This document provides technical best practices on handling small scale malware-related activity. 3 Pages (20-998)

CYBERSECURITY COUNSELING FOR IS & IT. This presentation given at the 2020 NOREX International Roundtable highlights cybersecurity issues and navigating away from cybersecurity make-believe. 24 Pages (20-956)

CYBERSECURITY INCIDENT RESPONSE PLAN. This procedure defines standard methods for identifying, containing, eradicating, and documenting the response to computer-based information security incidents. 20 Pages (20-845)

CYBERSECURITY FRAMEWORK. The following cybersecurity risk management framework ensures proper controls and proper mitigation steps are in place. 10 Pages (20-782)

SECURITY INCIDENT RESPONSE PLAN. This emergency operations & disaster preparedness plan explores response teams, mitigation, and recovery. 8 Pages (20-732)

CYBERSECURITY INCIDENT RESPONSE. This procedure and checklist describe processes for responding to potential information security events. 4 Pages (20-589)

CYBERSECURITY POLICY. This policy is for the development and maintenance of the information security environment and development of IT requirements that are reliable, secure, and predictable. 3 Pages (20-588)

CYBER RISK ASSESSMENT FORM. This form should help identify and document security control deviation as well as a plan of action to remediate the risk. 3 Pages (20-513)

DATA ACCESS & MANAGEMENT REQUIREMENTS. The issues of data and information security are discussed and include topics such as confidentiality, cyber security, and disaster recovery between clients and vendors. 4 Pages (20-364)

CYBERSECURITY ASSESSMENT. The Cybersecurity Assessment Tool helps financial institutions identify risks, assesses preparedness, and helps inform their risk management strategies. 39 Pages (20-252)

CYBER ATTACK TABLETOP EXERCISE. Performing this exercise will enhance preparedness, cyber readiness, and resiliency by testing the ability to comprehend effective response and recovery efforts needed during a cyber attack scenario. 22 Pages (20-234)

CYBER CRISIS MANAGEMENT SCENARIO. A discipline of Continuity Management, Crisis Management includes business & systems recovery. A strong program will help manage a crisis such as a cyber attack. 17 Pages (50-231)

CYBER ATTACK SCENARIO. Following is a cyber attack scenario for preparatory purposes. 17 Pages (50-230)

BREAKING THE CYBER CHAIN. Looking at security as a chain of events can give a different perspective on cybersecurity. This presentation describes breaking the chains of Ransomware, egress access, and encryption. 22 Pages (50-209)

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)

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)

DISASTER RECOVERY / BUSINESS CONTINUITY TRANSCRIPT. NOREX Members discussed best practices conducting Business Impact Analysis, addressing cyber-resilience for DR and BC, determining appropriate recovery time objectives and recovery point objectives, testing and training users, testing disaster recovery plans, and the use of vendors for DR. 16 Pages (NV2379)

MANAGING PRIVACY REGULATIONS TRANSCRIPT. NOREX Members discussed best practices to manage privacy regulations, assigning internal accountability / responsibility, defining private data, vendor contract review and protection assurance, utilizing a blockchain to enhance security integrity, and user education of and adherence to privacy policies. 16 Pages (NV2376)

CONSTRUCTION INDUSTRY – IT PROJECT MANAGEMENT. 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)

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)

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)

PATCH MANAGEMENT TRANSCRIPT. Member organizations share knowledge and many best practices / experiences regarding all aspects of patch management during this January 2021 WebForum. Several patching tools, poll results, and a lively chat section is included. 26 Pages (NV2352)

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)

MULTI-FACTOR AUTHENTICATION, SINGLE SIGN-ON, AND PASSWORD MANAGEMENT TRANSCRIPT. Members participate in a vigorous password management, SSO, and MFA discussion in December, 2020. Several products, links, polls, and experiences / strategies surrounding this important area of IT security are included. 21 Pages (NV2348)

BACKUP / RECOVERY TRANSCRIPT. Assuring that lost data can be accessed is a key factor to assuring businesses run smoothly. This discussion on this important task includes strong conversations around Veeam as a tool and its role in backing up Exchange. 10 Pages (NV2344)

ANTIVIRUS AND FIREWALLS TRANSCRIPT. In October 2020, organizations review antivirus and firewall standards, tool recommendations, potential new approaches / strategies regarding mobile device and the “new normal” of an increased remote workforce. A variety of polls are included. 18 Pages (NV2343)

ENDPOINT SECURITY TRANSCRIPT. NOREX members discussed different Endpoint Protection and Endpoint Detection & Response tools and strategies during this September, 2020 WebForum. Significant take-aways include the widespread use of SentinelOne, and the idea of using an analytics tool to analyze data generated by an EDR, rather than personnel. 15 Pages (NV2340)

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)

BI / DATA ANALYTICS TRANSCRIPT. NOREX Members discuss Business Intelligence and Analytics processes and tools during this August 2020 WebForum. 19 Pages (NV2337)

SECURITY: MOBILE DEVICES TRANSCRIPT. In August 2020, organizations discuss strategies and solutions used to address mobile device security. Several polls are included. 11 Pages (NV2334)

BUDGETING / COST SAVING MEASURES TRANSCRIPT. NOREX member discuss 2021 budget strategies and forecast in July 2021. Several polls and discussion on the COVID-19 impact on both decreased and increased spending is included. 17 Pages (NV2333)

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

SUPPORTING PARTIAL OFFICE AND WORK FROM HOME TRANSCRIPT. NOREX Members organizations compare strategies and experiences in managing / preparing for the look of the future office during this June 2020 session. 21 Pages (NV2328)

AZURE / AWS / GOOGLE ENTERPRISE CLOUD USAGE TRANSCRIPT. NOREX Members discuss the usage of Microsoft, Amazon and Google cloud services during this June 2020 WebForum. 20 Pages (NV2325)

SECURITY COMPLIANCE ISSUES TRANSCRIPT. NOREX Members strategize and discuss a variety of security compliance best practices, technologies, lessons learned and more during this June 2020 WebForum. 21 Pages (NV2324)

ASSET MANAGEMENT / PROCUREMENT FOLLOWING COVID-19 TRANSCRIPT. NOREX Members discuss ITAM strategies and tools in light of the COVID-19 Pandemic during this May 2020 WebForum. 20 Pages (NV2323)

COVID-19: BRINGING WORKFORCE BACK TRANSCRIPT. Organizations are currently working on how and when to move staff back to the office after the COVID-19 pandemic shutdown. Among the decisions to be made are whether to return the full or partial staff to the office. During this WebForum, NOREX Members and guests discussed options, resources, and lessons learned regarding equipment returns, social distancing in the office, government requirements and guidelines, stipends for employees, work prioritization, remote work tools, sanitizing, restrictions, and temperature scanning in the workplace. This transcript includes discussion about keeping the workforce safe after returning to the office, as well as a robust chat log conversation. 53 Pages (NV2321)

PATCH MANAGEMENT TRANSCRIPT. During this session, NOREX Members and guests discussed patch management automation, delays, tools, scheduling, solutions, and patch frequency. 16 Pages (NV2317)

CLOUD FIRST APPROACH / STRATEGY TRANSCRIPT. From key factors that drive usage to the cloud, adoption, moving existing applications, security measures, agnostic vs. native, the cloud Center of Excellence, and more are covered in this April, 2020 discussion. Polls and member chats are included. 28 Pages (NV2316)

COVID-19 PANDEMIC: RESPONSE, LESSONS LEARNED, WHAT'S NEXT? TRANSCRIPT. Members discuss how the organization has responded to the impact to the pandemic crisis. Lessons learned on supporting WFH from a technical, hardware, security and team engagement / collaboration, and what is next perspective are shared. Polls, links, and a lively chat section are included in this April, 2020 transcript. 28 Pages (NV2315)

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)

PREPARATION FOR A REMOTE WORKFORCE TRANSCRIPT. With the onset of COVID-19 and the need for distancing, aggressive remote workforce processes are in place for most NOREX Member organizations. NOREX hosted this discussion on March 17, 2020 with over 200 participants. This transcript includes a very active chat log conversation, results from polls taken, and the takeaways we received from those who completed an evaluation. 48 Pages (NV2313)

CHANGE MANAGEMENT TRANSCRIPT. NOREX hosted this Change Management discussion in March, 2020 with 60+ Members discussing new change management practices and trends as many embrace agile, lean, digital adoption and more. 17 Pages (NV2311)

ENDPOINT DETECTION / PREVENTION / RESPONSE TRANSCRIPT. Member organizations discuss Endpoint Detection / Prevention / Response during this March, 2020 WebForum. Several polls and a variety of products / solutions in use are included. 19 Pages (NV2310)

EMPLOYEE ONBOARD / OFFBOARD IT ISSUES TRANSCRIPT. What is the corporate lead time to setup new accounts? Who is responsible for opening onboarding tickets; training; off boarding best practices and the solutions / tools to assist with automation are included in this discussion. Polls, a lively chat and BYOD / MDM best practices are included in this March 2020 transcript. 30 Pages (NV2309)

2020 IT SECURITY INITIATIVES TRANSCRIPT. What are member organizations top IT security initiatives for 2020? This January 2020 discussion is packed with security plans, strategies, polls, links to solutions / tools, a lively chat section, and much more. 27 Pages (NV2303)

DISASTER RECOVERY / BUSINESS CONTINUITY TRANSCRIPT. This December 2019 discussion begins with best practices in conducting the Business Impact Analysis (BIA) and continues with a variety of DR and BC topics, solutions, polls, chats, and more. 17 Pages (NV2301)

WINDOWS 7 TO 10 UPGRADE TRANSCRIPT. NOREX Members discuss experiences and recommendations for the move from Windows 7 to Windows 10 during this November 2019 WebForum. 14 Pages (NV2300)

INCIDENT MANAGEMENT TRANSCRIPT. NOREX Members dedicate this November 2019 session to the processes, tools, best practices and general experiences with incident management. 15 Pages (NV2299)

PATCH MANAGEMENT TRANSCRIPT. NOREX Members share their patching schedules for routine and critical system patching and discuss tools used for applying patches during this November 2019 WebForum. 15 Pages (NV2298)

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)

SECURE CODING AND TESTING TRANSCRIPT. NOREX members discuss the procedures and tools recommended to ensure secure application development during this October 2019 WebForum. 17 Pages (NV2292)

ANTIVIRUS FILTERS AND FIREWALLS TRANSCRIPT. In October 2019, participants inquire and share their experiences and research on anti-virus filtering and firewall tools. Several polls identify trends, opinions and strategies to combat spam and virus infection. 21 Pages (NV2291)

ENTERPRISE STORAGE SOLUTIONS TRANSCRIPT. NOREX members discuss current storage trends including usage of flash, cloud options, modern data protection, automation and artificial intelligence during this September 2019 WebForum. 10 Pages (NV2289)

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)

DOCUMENT MANAGEMENT TRANSCRIPT. NOREX members share experiences selecting, implementing and managing Document Management systems during this September 2019 WebForum. 18 Pages (NV2286)

MULTI-FACTOR AUTHENTICATION AND SINGLE SIGN-ON TRANSCRIPT. NOREX members share recommendations for the adoption of MFA and SSO processes and tools during this August 2019 WebForum. 22 Pages (NV2285)

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)

IT ISSUES SPECIFIC TO THE EDUCATION INDUSTRY. NOREX participants discuss Higher Education issues, strategies and products used during this August 2019 session. 11 Pages (NV2282)

CYBERSECURITY TRANSCRIPT. This August, 2019 discussion is filled with member best practices, product experiences, and lessons learned on all aspects of cybersecurity. Several polls are included. 24 Pages (NV2281)

PRIVILEGED ACCESS MANAGEMENT TRANSCRIPT. NOREX members discuss the implementation and of Privileged Access Management procedures and tools during this July 2019 WebForum. 14 Pages (NV2278)

O365 NEW FEATURES / INITIATIVES TRANSCRIPT. Members share experiences with the implementation of various Microsoft Office 365 services and features including PowerBI, SharePoint, Skype for Business and Teams during this June 2019 WebForum. 32 Pages (NV2275)

BUSINESS INTELLIGENCE TRANSCRIPT. Members share recommendations on starting a BI practice and experiences with various BI tools during this June 2019 WebForum. 21 Pages (NV2274)

SECURITY FRAMEWORKS TRANSCRIPT. NOREX members discuss procedures and strategies regarding Security Frameworks during this May 2019 session. 19 Pages (NV2272)

BACKUP / RECOVERY TRANSCRIPT. Members share experiences with the leading backup and recovery tools during this May 2019 WebForum. 12 Pages (NV2270)

NETWORK PERFORMANCE AND CAPACITY PLANNING TRANSCRIPT. Members discuss strategies for improving network performance with an emphasis on proprietary and open source monitoring tools during this April 2019 WebForum. 21 Pages (NV2265)

DISASTER RECOVERY TRANSCRIPT. Topics of this March 2019 session include recovery approaches such as on-prem vs. DR-as-a-Service, backup and recovery tools, testing strategies and Business Continuity considerations. 20 Pages (NV2264)

DATA LOSS PREVENTION (DLP) TRANSCRIPT. Getting started with DLP, DLP attributes, solutions used, cloud impact, data classification, and more are discussed during this March 2019 WebForum. 17 Pages (NV2263)

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)

GLOBAL IT ISSUES TRANSCRIPT. NOREX members share strategies and solutions used to support technologies globally during this February 2019 WebForum. 13 Pages (NV2260)

ENDPOINT SECURITY TRANSCRIPT. NOREX members discuss procedures and tools used in endpoint security during this February 2019 session. 22 Pages (NV2258)

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)

SECURITY INITIATIVES FOR 2019 TRANSCRIPT. This January, 2019 security discussion covers a wide range of member security initiatives planned for this year and/or already implemented. Many links, polls and multiple chat discussions are included. 33 Pages (NV2253)

SELECT: ENDPOINT SECURITY TRANSCRIPT. NOREX Select Members from Fortune / Forbes 1000 organizations discussed endpoint security initiatives, best practices, lessons learned, locking down devices on terminated remote workers and vendors, BYOD endpoint protection, solution management, endpoint security tools, and User Entity Behavioral Analytics. 22 Pages (NS215)

QUICK POLL RESULTS: SIEM. In July 2021, 114 NOREX Member organizations responded to a poll regarding Security Information and Event Management which provides organizations with next-generation detection, analytics and response. Questions were based on SIEM / Log Management and endpoint security solutions. 2 Pages (NP2384)

QUICK POLL RESULTS: ELECTRONIC COMMUNICATION RETENTION. In April 2021, 103 NOREX Member organizations responded to a poll regarding electronic communication retention. Questions were based on standard retention policies for email, instant messaging / chat, text messaging, video / audio recording, and also included retention tools being used. 2 Pages (NP2370)

GOVERNMENT: MS365 ADOPTION TRANSCRIPT. NOREX Members from Government agencies share strategies on the adoption of Microsoft's M365 licencing 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: NAVIGATING INTERNATIONAL / GLOBAL IT ISSUES DURING A PANDEMIC TRANSCRIPT. During this CIO call, NOREX Members and guests shared experience and ideas on global office management, particularly in Asia. They discussed differences in products, regulations, firewalls, long distance connectivity, and collaboration tools. 21 Pages (CV074)

CIO: REMOTE WORKFORCE / WORK-FROM-HOME TRANSCRIPT. The benefits and concerns of supporting a remote workforce and a work-from-home program are a hot topic for IT executives. In December 2019, NOREX members discuss experiences, recommendations, policy, tools to support, and general consideration when offering employee remote workforce / WFH programs. 26 Pages (CV073)

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)

Encryption

ACCEPTABLE ENCRYPTION POLICY. This policy limits the use of encryption to those algorithms that have received substantial public review and proven effectiveness, and provides direction to ensure that Federal regulations are followed. 1 Page (20-1035)

HTTPS / SSL INSPECTION. This presentation provides information on recognizing when, why, and how inspection of HTTPS traffic should be done. 14 Pages (20-741)

AUTOMATED SSL INSPECTION NOTICE. This is an example of a notification for a planned and automatic SSL encrypted data inspection. 1 Page (20-740)

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

ACCEPTABLE USE & SECURITY STANDARD. This policy describes authorized usage, outlining responsibilities related to electronic equipment, software, and networks. Maintaining security of communication networks, proprietary information, and data security essential to daily operations is also addressed. 4 Pages (20-604)

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)

E-COMMUNICATION TOOLS STANDARD. E-mail, encryption, Instant Messenger, and electronic communications record retention standards are outlined here. 1 Page (20-305)

Incident Management

SECURITY INCIDENT EMAIL TEMPLATE. This template is used to inform employees of a potential email security incident and how to utilize a company-subsidized account with a third-party security provider. 1 Page (20-1049)

INCIDENT RESPONSE PLAN. This plan outlines general guidelines and procedures to protect from and respond to unforeseen events and incidents. 6 Pages (20-992)

INCIDENT RESPONSE PROCEDURE. This document outlines a policy for incident response capabilities that are used to monitor security incidents, determine the magnitude of the threat, and respond to these incidents. 4 Pages (20-922)

TABLETOP EXERCISE AFTER-ACTION REPORT. The following is an evaluation template of how a tabletop exercise provided insight into how effective the security incident response plan is in responding to a security incident. 5 Pages (20-900)

TABLETOP EXERCISE PARTICIPANT GUIDE. This is a guide for participants in a tabletop exercise conducted to evaluate response procedures, communication, and decisions. 5 Pages (20-899)

TABLETOP EXERCISE FACILITATOR GUIDE. To validate your company's security incident response plan, a tabletop exercise will be conducted to evaluate response procedures, decisions, and communication. 6 Pages (20-898)

TABLETOP EXERCISE INSTRUCTION. This instruction will help you design, develop, conduct, and evaluate a security incident response plan tabletop exercise. 7 Pages (20-897)

INCIDENT RESPONSE PLAN. This response plan describes actions that would be taken after a known or suspected information security incident affected its technology system(s) or data. 9 Pages (20-857)

INCIDENT MANAGEMENT HIGH LEVEL DESIGN. This document provides a high level or management view of the Incident Management (IM) Process within an IT department. 24 Pages (20-822)

INCIDENT MANAGEMENT PROCESS ASSESSMENT. The objectives of this exercise are to document good practice that is performed across all process stakeholders and to identify gaps for improvement. 4 Pages (20-821)

MAJOR INCIDENT POLICY. Processes and procedures related to a major incident are described in this policy. 4 Pages (20-820)

INCIDENT PRIORITY MODEL. This model helps designate the impact's degree of failure, urgency, priority, and cost. 6 Pages (20-819)

SECURITY INCIDENT RESPONSE PLAN. This emergency operations & disaster preparedness plan explores response teams, mitigation, and recovery. 8 Pages (20-732)

INCIDENT MANAGEMENT. This policy ensures that all information technology security incidents are properly reported and responded to in a timely manner. 3 Pages (20-634)

REPORTING SUSPICIOUS EMAIL. This document tells us how to forward suspicious email, as an attachment, to the security department for review. 7 Pages (20-596)

EMAIL AND INFORMATION SECURITY. This is a brief explanation of what employees should do if they believe they've received malicious email. 2 Pages (20-595)

INCIDENT RESPONSE POLICY. This policy is for communication, response, mitigation, and remediation of IT related incidents that impact or threaten computing equipment, data, or networks. 3 Pages (20-551)

INCIDENT RESPONSE PLAN. An IRP is a formal roadmap to follow when handling suspected intrusions, system misuse, a cyber incident, or any incident where unauthorized access to confidential information has been detected or suspected. 26 Pages (20-382)

INCIDENT REPORT LOG. This document provides the guidelines for the creation, maintenance, management, and secured storage of the Incident Report Log (IRL). 2 Pages (20-350)

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)

INCIDENT RESPONSE PLAN. The plan will facilitate the security response and remediation process to ensure the least amount of potential damage to systems, networks, members, and business reputation. 8 Pages (20-098)

SECURITY INCIDENT RESPONSE PLAN. This response plan describes actions that a company would take after a known or suspected information security incident affecting its technology system(s) and/or data. 18 Pages (20-053)

INCIDENT RESPONSE STANDARD. This Incident Response Standard provides a documented approach for handling potential threats to company computers, systems, and data. 22 Pages (50-293)

WEEKLY TREND INCIDENT REPORT. Weekly ITS critical and high incident reports are demonstrated as enterprise-wide and divisional categories. 7 Pages (50-258)

MONTHLY INCIDENT REPORTS. Following are examples of monthly incident reports from various locations for a one to two year period. 15 Pages (50-257)

INCIDENT RESPONSE PLAN. This document details the procedure to follow when a potential incident is identified. An incident may be a malicious code attack, unauthorized access to systems, unauthorized utilization of services, denial of service attacks, general misuse of systems, or sabotage/theft. 33 Pages (50-252)

ROOT CAUSE ANALYSIS TECHNIQUES. Using disciplined problem solving techniques can help manage a problem's lifecycle and reduce its impact. 29 Pages (50-210)

SAMPLE PARETO DASHBOARD. The sample Pareto view provides insight for incident ticket quantity and age. The chart groups incident tickets into two primary views (Parent Groups IMS & AMS). 2 Pages (50-183)

AFTER ACTION REVIEW TIMELINE. The following outlines a meeting between IS and Business stakeholders to review unplanned events discussing the cause, resolution, and lessons learned. 2 Pages (50-182)

Mobile Computing

REPORTING MOBILE DEVICE LOSS. This procedure provides for timely reporting of loss or theft of company-owned mobile devices. 3 Pages (20-853)

MOBILE DEVICE SECURITY. Rules and procedures involving employee mobile devices are examined in this policy. 5 Pages (20-844)

MOBILE POLICY AND PROCEDURE. This policy aims to protect the integrity and security of confidential client and business data within the infrastructure through secure processes involving mobile devices. 6 Pages (20-827)

INFORMATION SECURITY PROGRAM. This ISP is designed to protect against anticipated internal and external threats or hazards to information security or integrity, and against unauthorized access to or use of such information. 54 Pages (20-742)

MOBILE DEVICE PROTECTION. The objective of this policy is to protect data stored on company issued mobile devices and to prevent the theft or loss of those mobile devices. 2 Pages (20-636)

MOBILE ACCESS PROCEDURE. This procedure provides direction, standards, and steps for connecting mobile devices to the data network and information resources. 6 Pages (20-585)

MOBILE DATA SECURITY ACKNOWLEDGEMENT. Following is a template for an agreement between the organization and the employee who uses company-issued devices such as laptops or tablets. 1 Page (20-571)

VIDEO SURVEILLANCE SYSTEM SOW. The purpose is to procure a high quality, reliable and effective mobile surveillance system that will monitor and record interior and exterior events. 8 Pages (20-564)

MICROSOFT CLOUD SECURITY. These slides represent a company making a secure transition to the cloud. 25 Pages (20-534)

MOBILE DEVICE POLICY. The guiding purpose of this policy is to ensure that mobile devices are appropriately used, while maintaining security and confidentiality. 4 Pages (20-420)

CORPORATE & REMOTE SECURITY. The following policy documents standards and practices for onsite and remote location security badge access systems. 2 Pages (20-377)

Password

PASSWORD VAULT SCORING MATRIX. Several password vault solutions are compared using features such as quality, ease of use, automated sync, security, and integration. 1 Page (20-1096)

IT PASSWORD STANDARD. This standard describes policy on password and secure passphrase creation and maintenance. 4 Pages (20-989)

EXPIRED PASSWORD. Follow this process to reset your expired password or connect with the network when you're offsite. 2 Pages (20-832)

DESKTOP PASSWORD POLICY. This policy governs the length, complexity, age, and lockout thresholds for IT passwords. 2 Pages (20-751)

PASSWORD POLICY. The requirement is to set a consistent standard concerning the appropriate password creation, usage, storage, and overall company stance on passwords. 7 Pages (20-557)

PASSWORD MANAGEMENT POLICY. The password management policy and procedures is part of the security management process for Information Technology resources. 3 Pages (20-404)

PCI

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)

CARDHOLDER DATA ENVIRONMENT. The diagrams herein identify all connections between the cardholder data environment and other networks, including any wireless networks. 8 Pages (20-278)

APPLICATION SECURITY POLICY. This document outlines the policies for cardholder data environment application security. 8 Pages (20-277)

Plans and Manuals

COVID-19 RESPONSE TELEWORK SURGE CHECKLIST. This document is designed as a quick reference for considering important factors in a teleworking strategy that minimizes downtime and latency. 10 Pages (20-877)

PANDEMIC PREPAREDNESS PLAN. Here is a flexible guide for responding to the problems associated with a pandemic influenza outbreak. 31 Pages (20-859)

PANDEMIC PLAN: ISOLATION GUIDE. This document provides a flexible plan for the isolation of staff in the event of an outbreak of illness such as influenza. 3 Pages (20-858)

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)

INFORMATION SECURITY PROGRAM. This ISP is designed to protect against anticipated internal and external threats or hazards to information security or integrity, and against unauthorized access to or use of such information. 54 Pages (20-742)

SECURITY INCIDENT RESPONSE PLAN. This emergency operations & disaster preparedness plan explores response teams, mitigation, and recovery. 8 Pages (20-732)

BUSINESS CONTINUITY PLAN. The following BCP template is a guide for creating your own continuity plan to preserve critical processes and operations. 14 Pages (20-684)

BUSINESS CONTINUITY MANAGEMENT. Included in this Business Continuity Plan are policies, procedures, and organization charts for crisis management and disaster recovery. 93 Pages (20-682)

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)

IT CLOUD STRATEGY. Cloud services include Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), and this strategy focuses on productivity applications as well as data protection. 23 Pages (20-587)

CLOUD COMPUTING STRATEGY. This presentation offers an overview of cloud computing and what comprises a beneficial cloud computing service. 15 Pages (20-586)

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)

ENTERPRISE SECURITY ARCHITECTURE. Enterprise Security Architecture ensures that information and information systems are protected. 27 Pages (20-207)

INFORMATION SECURITY PROGRAM. This ISP is designed to protect against any anticipated internal and external threats or hazards to the security or integrity of such information. 47 Pages (20-100)

DDoS MITIGATION PLAN. A Distributed Denial of Service (DDoS) attack can be a website shutdown to interrupt a business, holding a business hostage while demanding payment to release the website, or overloading a firewall so the actor(s) can try penetrating the firewall & implanting malware or a backdoor into the victim's network. 7 Pages (20-099)

IT SECURITY MANUAL. This is an enterprise level policy to guide the maintenance of an environment across all departments and agencies. 6 Pages (20-068)

PANDEMIC BUSINESS CONTINUITY PLANNING STRATEGY. This document describes a strategy for sustaining utility operations in the event of an influenza pandemic, based upon previous world pandemic events. This strategy can be updated and applied to potentially pandemic situations. 36 Pages (47-494)

IT PANDEMIC INCIDENT RESPONSE PLAN. This document serves as protection for employees, customers, assets & information, and will minimize restoration time in the event of a pandemic. 28 Pages (47-493)

ROBOTIC PROCESS AUTOMATION. Offered at a recent NOREX workshop, this presentation offers a discussion about RPA and its security implications. 15 Pages (50-291)

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

ADAPTIVE SECURITY. This approach to security architecture integrates predictive, preventive detective, & response capabilities. 5 Pages (50-203)

Policies & Procedures

IT SECURITY POLICY. This document is an overview of the security requirements of company systems. Additionally, it describes controls implemented to meet those requirements. 8 Pages (20-1066)

WIRELESS SECURITY POLICY. This policy prohibits access to company networks via unsecured wireless communication mechanisms, and covers all wireless data communication devices. 2 Pages (20-1036)

REMOTE ACCESS SECURITY POLICY. This policy defines standards for network connection from any external host. These standards minimize the potential exposure to damages which may result from unauthorized use of company resources. 2 Pages (20-1033)

CHANGE MANAGEMENT AND CONTROL POLICY. This policy provides standardized methods and procedures to meet change management requirements supporting IT operations. 5 Pages (20-1027)

INFORMATION TECHNOLOGY USE. This Information Resources policy preserves confidentiality, integrity, and availability of systems, applications, and data. 8 Pages (20-995)

IT SECURITY DEFENSE POLICY. Passive Defense serves as the foundation of protecting networks and systems. This policy follows deployment of security controls to the baseline IT architecture to provide defense or insight against threats. 6 Pages (20-975)

VENDOR RISK MANAGEMENT. This procedure specifies security requirements for IT products and services in which data is stored, processed, or transmitted by entities not under direct control of your organization. 4 Pages (20-974)

IT SECURITY POLICY. This policy informs staff of technology and information asset protection requirements and describes IT responsibilities and privileges. 5 Pages (20-973)

IDENTITY & ACCESS MANAGEMENT POLICY. The objective of this policy is to ensure existence of adequate controls to restrict access to systems and data for user, shared, privileged, and service accounts. 3 Pages (20-972)

SECURITY INCIDENT RESPONSE & INVESTIGATION. This procedure describes how to respond to IT security incidents and investigate causes in order to stop the problem, prevent future incidents, and identify areas of weakness or vulnerability. 10 Pages (20-971)

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)

DATA CLASSIFICATION STANDARD. This is a draft of a standard that creates a common set of terms for categorizing and securing information. 2 Pages (20-918)

DATA SECURITY CLASSIFICATION. In this document, distinct handling, labeling, destruction, and review procedures are established for each security classification. 1 Page (20-917)

INFORMATION TECHNOLOGY POLICY. The purpose of this document is to establish and document the details of the system security reviews. 26 Pages (20-912)

NETWORK OPERATIONS CHECKLISTS. Included are daily and weekly network operations security health checklists. 1 Page (20-904)

IT LOGICAL SECURITY POLICY. This document describes the procedure for the application of logical security measures to protect information systems and data. 7 Pages (20-875)

MOBILE DEVICE SECURITY. Rules and procedures involving employee mobile devices are examined in this policy. 5 Pages (20-844)

VIDEO SECURITY SYSTEMS STANDARDS AND GUIDELINES. In order to provide all employees a safe and secure working area, this company supports the implementation of Video Security Systems that include a specific set of coverage areas in all facilities. 5 Pages (20-767)

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)

PROCUREMENT SECURITY REQUIREMENTS. Security requirements for on- and off-premise systems, data use, login, and application use are described in this document. 3 Pages (20-722)

ACCESS & IDENTIFICATION BADGE POLICY. The employee ID badge provides a unique identifier that verifies a person's authorization to be in restricted or non-public facility spaces. This policy describes issuance and use of ID badges. 7 Pages (20-690)

BUSINESS CONTINUITY MANAGEMENT POLICY. Effective contingency planning can minimize the impact of a disaster or threat. This document provides planning and program guidance for implementing a Business Continuity Plan (BCP). 17 Pages (20-685)

VIDEO RETENTION & DISTRIBUTION. This administrative policy describes maintenance of video recordings on all modes and how such recordings are preserved, reviewed, and distributed. 9 Pages (20-649)

CLOSED CIRCUIT TV PROCEDURES. The CCTV system is used to monitor public areas in order to deter crime, scan for safety concerns, and to assist in providing a secure environment. This document provides guidance for CCTV use. 7 Pages (20-648)

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 CENTER SECURITY. This policy outlines Data Center rules and procedures. 5 Pages (20-643)

VIRUS PREVENTION POLICY. This policy is designed to ensure that IT resources and systems employ effective anti-virus and anti-malware detection software. 2 Pages (20-633)

ACCEPTABLE USE & SECURITY STANDARD. This policy describes authorized usage, outlining responsibilities related to electronic equipment, software, and networks. Maintaining security of communication networks, proprietary information, and data security essential to daily operations is also addressed. 4 Pages (20-604)

SECURITY AWARENESS TRAINING POLICY. The information security awareness program ensures that all employees achieve and maintain at least a basic level of understanding of information security matters, ethics, and acceptable behavior. 3 Pages (20-603)

ACCESS & USAGE POLICY. General policy on computer (and other electronic systems) access and usage as it relates to the security management process is described. 4 Pages (20-593)

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

NETWORK SECURITY POLICY. This policy establishes administrative direction, procedural requirements, and technical guidance to ensure the appropriate protection of information handled by computer networks.
12 Pages (20-561)

OPERATING SYSTEM SECURITY POLICY. The scope of this policy encompasses all operating systems, including but not limited to, main frame, network, Microsoft Windows, Unix, Linux, and SQL Server implementations. 1 Page (20-547)

SECURITY EXCEPTION FORM. This form manages exceptions to Information Security policies and standards. 2 Pages (20-512)

IT SECURITY POLICY. This policy describes controls, that when implemented by supporting standards and procedures, are designed to move any associated risks to an acceptable level. 20 Pages (20-487)

ACCESS CONTROL POLICY. This complication of future implementations center on user authentication, access control, identification procedures, and more. 12 Pages (20-486)

INFORMATION SERVICES SECURITY POLICY. The policy provides the framework to ensure protection of IT assets and to allow the use, access, and disclosure of such information only in accordance with appropriate standards, laws, and regulations. 18 Pages (20-477)

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

AUDIOCODES MAINTENANCE & SUPPORT GUIDELINES. Security patches and cumulative updates for AudioCodes Gateways, Survivable Branch Appliances (SBA), and SmartTAP Recording Solution are some of the components in need of maintenance and support. 2 Pages (20-456)

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)

IDENTITY MANAGEMENT & ACCESS CONTROL POLICY. This policy establishes procedures controlling system access and defining the security management process for information technology resources. 4 Pages (20-402)

WEB APPLICATION SECURITY STANDARDS. This document provides technical standards to guide the specification, design, procurement, configuration, and administration of web applications. 6 Pages (20-371)

COMPUTER CRIMES POLICY. The company's policy on computer misuse and crime is addressed here, including examples of such and the process of reporting such crimes. 4 Pages (20-319)

SECURITY MONITORING POLICY. This policy defines rules & requirements for securing & protecting electronic communications systems and defines requirements for Information Security (InfoSec) monitoring, Cybersecurity, and Network security. 3 Pages (20-317)

IT USE POLICY. This policy provides standards for the acceptable use of company IT resources, and is designed to prevent use that may be illegal, improper, abusive, or which may have an adverse impact on the company or its IT resources. 9 Pages (20-303)

IT SECURITY POLICY. Standards for the maintenance & protection of the IT infrastructure, including all equipment, software, and systems owned, operated, or maintained by or on behalf of the company. 8 Pages (20-302)

PHYSICAL ACCESS POLICY. This document outlines the policies for providing physical access to system components. 5 Pages (20-282)

IT SECURITY POLICY. This policy establishes standards for maintenance & protection of the IT infrastructure, including all equipment, software and systems owned, operated, or maintained by or on behalf of the IT Department. 8 Pages (20-266)

DATA SECURITY POLICY. In this policy, procedures are set forth to ensure the security & confidentiality of personal information, protect against threats to security and integrity, and protect against unauthorized access to such information. 59 Pages (20-241)

MEDIA HANDLING STANDARD. This Standard protects physical Information System Media from unauthorized disclosure, modification, removal, or destruction. 2 Pages (20-149)

ACCEPTABLE USE OF TECHNOLOGY. Proper and acceptable use of technology resources are explained in the following document. 6 Pages (20-069)

NETWORK ACCESS SECURITY POLICY. Described here is official policy on network access, security, and electronic communication. 9 Pages (20-044)

INFORMATION ASSET PROTECTION. The following is the procedure for requesting access to company systems and applications and their security. 11 Pages (20-042)

WORK-FROM-HOME SECURITY GUIDANCE. Use the guidance provided in this document to improve the security of WFH. 4 Pages (50-323)

ELECTRONIC COMMUNICATIONS POLICY. This policy guides use of company systems (computers, phones email, software, applications, smart devices, removable media, etc.), internet use, and protection of information on company systems. 5 Pages (50-322)

SOFTWARE DEVELOPMENT SECURITY POLICY. This policy provides guidance on preserving confidentiality, integrity, and availability of confidential information. 5 Pages (50-284)

SECURITY POLICY EXCEPTION. This form is used to manage exceptions to any Information Security or Systems policy or standard due to operational constraints, technical limitations, legal requirements or other issues. 2 Pages (50-271)

Polls

MEMBER VENDOR RATINGS: MULTI-FACTOR AUTHENTICATION. This Multi-Factor Authentication Tools and Solutions poll resulted in 30 products being rated. 6 Pages (NR009)

MEMBER VENDOR RATINGS: ENDPOINT SECURITY. This Endpoint Security Tools and Solutions poll resulted in 50 products being rated. 5 Pages (NR008)

MEMBER VENDOR RATINGS: NETWORK SECURITY. This Network Security Tools and Solutions poll resulted in 65 products being rated. 5 Pages (NR007)

MEMBER VENDOR RATINGS: PATCH MANAGEMENT. This Patch Management Tools and Solutions poll resulted in 24 products being rated. One hundred and thirty members responded. 3 Pages (NR003)

MEMBER VENDOR RATINGS: PASSWORD MANAGEMENT. This Password Management Tools and Solutions poll resulted in 31 products being rated. One hundred and thirty members responded. 3 Pages (NR002)

QUICK POLL RESULTS: SIMULATED PHISHING TESTS. In March 2020, nearly 200 NOREX members responded to a poll on simulated phishing test practices. Questions covered frequency and click rate of phishing tests and tools used. Key comments were given on what is done after repeated failed tests and effectiveness of security awareness training. 15 Pages (NP2312)

QUICK POLL RESULTS: WORK-FROM-HOME TRENDS. In October 2019, 200 NOREX members responded to a poll on Work-from-Home Trends. Questions covered organization's practices and policies on employees working from home. Key comments were given on what IT positions were allowed to work from home, when is it offered, what support employees receive and what benefits and negatives are seen from staff working from home. 14 Pages (NP2297)

QUICK POLL RESULTS: TECHNOLOGY & BUDGET TRENDS 2019. Member organizations participated in our Technology & Budget Trends poll in December 2018. This poll includes deployment plans, technology plans, cloud solutions, desktops/laptops, IT staffing/salaries, new technologies or applications implemented in 2018 and projects planned for 2019. 12 Pages (NP2252)

QUICK POLL RESULTS: SECURITY 2018. In August 2018, NOREX polled the membership on security issues. Topics addressed include phishing, multi-factor authentication, passwords, cybersecurity and cloud security. 15 Pages (NP2237)

REAL-WORLD IT TRENDS. The IT professionals that make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. Real-World IT Trends is a collection of the NOREX Member input captured in the first quarter of 2021 from Virtual Roundtable and WebForum polls. 55 Pages (DT2021-1)

YOUR DATA: 2020 REAL-WORLD IT TRENDS. The IT professionals that make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. Real-World IT Trends is a collection of the NOREX Member input captured in the first half of 2020 from Virtual Roundtables and WebForum polls. 61 Pages (DT2020-1)

YOUR DATA: 2019 REAL WORLD IT TRENDS. The IT professionals that make up NOREX realize the benefits of no vendor bias when analyzing IT polls and trends. Your Data is a collection of the real world member input captured in the second half of 2019 WebForum polls. 36 Pages (DT2019-2)

YOUR DATA: 2019 REAL WORLD IT TRENDS. The IT professionals that make up NOREX realize the benefits of no vendor bias when analyzing IT polls and trends. Your Data is a collection of the real world member input captured in the first seven months of 2019 WebForum polls. 25 Pages (DT2019-1)

RFP & Contracts

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)

SECURITY STANDARDS WORDING. This describes wording for information security requirements guidelines to be used for bids and RFP documents. 2 Pages (20-542)

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)

INFORMATION SECURITY REQUIREMENTS AGREEMENT. This ISR is an exhibit to the Master Services Agreement effective under which provider may be engaged from time to time to provide services. 5 Pages (20-538)

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)

RFP: MSSP. For the purpose of engaging into a partnership with a professional Managed Security Service Provider (MSSP) for security monitoring and other network & computing asset security services, this informal RFP has been issued. 9 Pages (20-412)

RFP: NETWORK FIREWALL & SECURITY APPLIANCE. A larger-scale network firewall & security appliance is needed to meet specific connection speeds, protection, filtering, and Ethernet interfaces. 5 Pages (20-379)

PRIVILEGED ACCESS AGREEMENT. This agreement includes acknowledgement of responsibilities, necessary clearances, and authorization for privileged access to systems. A non-disclosure certificate is also included. 3 Pages (20-362)

SECURITY CONSULTANT REQUEST. Various security tasks such as vulnerability assessment, penetration testing, awareness training, and incident response will need to be performed by the security consultant. 5 Pages (20-106)

RFI: EVENT MANAGEMENT SOFTWARE SOLUTION. This Request for Information is for those in the process of identifying Event Management Software vendors for an upcoming requirement. 5 Pages (20-095)

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

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

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)

Risk Assessment

IT VENDOR RISK MANAGEMENT PROCEDURE. This procedure specifies security requirements for acquisition of IT products and services in which data is stored, processed, or transmitted by an entity not under direct control. 4 Pages (20-1092)

SOFTWARE RISK ASSESSMENT. This document provides a standard procedure for reviewing software that is to be installed in the company environment. 7 Pages (20-996)

COMPLEXITY MATRIX & RISK PLAN TEMPLATE. Track the complexity and risk of the proposed plan using these PMO templates. 2 Pages (20-784)

VENDOR SECURITY ASSESSMENT. This questionnaire is about secure coding, incident response, confidentiality, and other aspects of vendor security. 2 Pages (20-683)

SECURITY QUESTIONNAIRE. Designed using the NIST guide, this questionnaire will help determine the level of risk and organization will incur using the provider in question. 32 Pages (20-584)

RISK REGISTRY DASHBOARD. This dashboard template logs impact area, source risk factors, description, probability, assessment, and response. 5 Pages (20-384)

RISK REGISTER TEMPLATE. This risk register contains typical risks that have been identified on previous projects, potential triggers, and possible responses. A contingency plan is also suggested. 5 Pages (20-383)

RISK APPETITE STATEMENT. This statement considers the most significant risks to which a financial institution is exposed and provides and outline of the approach to managing and mitigating those risks. 4 Pages (20-251)

IT RISK ASSESSMENT. This is a worksheet detailing external and internal threats as well as disaster risk factors. 3 Pages (20-250)

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)

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)

SOW: VULNERABILITY & PENETRATION TESTING. Vulnerability identification and analysis, physical security, authenticated and unauthenticated testing is examined in this SOW. 11 Pages (20-143)

ROOT CAUSE ANALYSIS. The description, principles, general process, benefits, common pitfalls, and examples of an RCA are provided in this presentation. 15 Pages (20-121)

SYSTEM OUTAGE ROOT CAUSE ANALYSIS. The following is a chart for recording details of a service desk ticket problem and the subsequent Root Cause Analysis (RCA). 2 Pages (20-120)

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)

CHANGE MANAGEMENT RISK ASSESSMENT. This simplified risk assessment is limited to a few questions and designed to be free from subjective responses. 1 Page (50-317)

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

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

OPERATIONAL READINESS INTAKE. This questionnaire provides an opportunity for each department to submit change requests in a timely and organized manner, so that they can be properly managed. 9 Pages (50-276)

RISK ASSESSMENT. The following risk assessment questions, submitted by three different member organizations, help assess the risk associated with technical changes. 3 Pages (50-221)

Security Awareness

SECURITY AWARENESS TRAINING POLICY. This policy ensures all employees understand security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior. 3 Pages (20-1048)

IT SECURITY FRAMEWORK. This security infographic provides an outline of IT security systems. 2 Pages (20-1040)

SECURITY TIPS: MEMBER PERSPECTIVES. Following are tips a NOREX member has shared regarding experiences with security awareness and resources. 2 Pages (20-614)

SECURITY AWARENESS TRAINING POLICY. The information security awareness program ensures that all employees achieve and maintain at least a basic level of understanding of information security matters, ethics, and acceptable behavior. 3 Pages (20-603)

SECURITY CONSULTANT REQUEST. Various security tasks such as vulnerability assessment, penetration testing, awareness training, and incident response will need to be performed by the security consultant. 5 Pages (20-106)

IT SECURITY: NATION STATE ACTORS. This presentation was given at a NOREX Security Workshop, and discusses advanced threats, nation states, attack tactics, and follow-up ideas. 22 Pages (50-265)

IT SECURITY TRENDS & TIPS. This is a member's perspective on the state of IT security, current threats, and technologies to apply. 25 Pages (50-228)

Security Charter & Framework

KEYS TO SECURITY OPERATIONS CHARTERS. The latest in SOC technology includes identifying access, communication, and using the right tools for the job. 15 Pages (50-365)

STRATEGIC PLAN OUTLINE. This outline aligns IT security strategy with business objectives while effectively managing risk and meeting compliance requirements. 13 Pages (50-352)

CYBERSECURITY FRAMEWORK. The following cybersecurity risk management framework ensures proper controls and proper mitigation steps are in place. 10 Pages (20-782)

IDENTITY & ACCESS MANAGEMENT SOLUTION. This template demonstrates how to select, acquire, and implement an Identity and Access Management (IAM) solution for single sign-on, universal directory, and adaptive multifactor authentication. 8 Pages (20-728)

PRIVILEGED ACCESS MANAGEMENT. The Information Services Security Team recommends procuring a solution that will allow implementation of privileged account control, least-privilege access on workstations, and password vaulting. 6 Pages (20-727)

PROCUREMENT SECURITY REQUIREMENTS. Security requirements for on- and off-premise systems, data use, login, and application use are described in this document. 3 Pages (20-722)

IT SECURITY CONTROL FRAMEWORK. This control framework provides management direction & support for information security. 4 Pages (20-706)

INFORMATION SECURITY ORGANIZATION STRUCTURE. Following a chart of IS organization is a detailed description of the allocation of information security responsibilities. 5 Pages (20-615)

PATCH MANAGEMENT SECURITY STANDARD. As set forth in this standard, the Patch Advisory Team meets monthly to ensure all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. 2 Pages (20-546)

SOW: VULNERABILITY & PENETRATION TESTING. Vulnerability identification and analysis, physical security, authenticated and unauthenticated testing is examined in this SOW. 11 Pages (20-143)

CLOUD SECURITY FRAMEWORK. This framework of steps procures a cloud service that meets information security policies, standards, and baselines. 7 Pages (50-347)

AWS CLOUD SECURITY STANDARD. This security standard provides the technical and operational security requirements for AWS hosted infrastructure and services. 21 Pages (50-308)

IT SECURITY CHARTER. The responsibilities of the IT Security Department are outlined in detail along with mission statements and department vision for security standards. 7 Pages (50-292)

CRISIS MANAGEMENT STEERING COMMITTEE CHARTER. The risk processes and responsibilities of a crisis management steering committee are outlined here. 2 Pages (50-229)

Staffing

NETWORK SECURITY ANALYST. 2 Pages (20-1031)

MANAGER: NETWORK OPERATIONS & SECURITY. 4 Pages (20-776)

IT SECURITY DIRECTOR. 2 Pages (20-526)

DIRECTOR OF IT SECURITY. 1 Page (20-523)

CLINICAL INFORMATICS SPECIALIST. 4 Pages (20-394)

JOB DESCRIPTION TEMPLATE. This template describes the essential functions of a position and gathers information to identify both common and unique requirements for all positions throughout the company.
8 Pages (20-170)

JUNIOR SECURITY ANALYST. 1 Page (20-169)

JUNIOR SECURITY ANALYST. 1 Page (20-166)

CHIEF INFORMATION SECURITY OFFICER. 3 Pages (20-079)

CYBER SECURITY OFFICER. 2 Pages (20-073)

SENIOR INFORMATION SECURITY ANALYST. 3 Pages (20-062)

IAM SYSTEMS ANALYST. 2 Pages (20-047)

IAM PROGRAM MANAGER. 2 Pages (20-046)

IAM SOLUTIONS ARCHITECT. 1 Page (20-045)

GRC MANAGER. 2 Pages (50-298)

SOFTWARE DEVELOPMENT ORG CHART. Organization of software development teams are shown in this example chart. 1 Page (50-288)

IDENTITY ACCESS MANAGEMENT ARCHITECT. 3 Pages (50-214)

IDENTITY ACCESS MANAGEMENT ENGINEER. 2 Pages (50-213)

IDENTITY MANAGEMENT ENGINEER. 1 Page (50-212)

Vendor Management

SaaS SECURITY CHECKLIST. Aspects of Software as a Service such as vendor policies, compliance requirements, security safeguards, and documentation are part of this checklist. 2 Pages (20-1095)

EMAIL SECURITY PRODUCT SCORESHEET. This chart provides a weighted comparison of several prominent email security products. 3 Pages (20-1044)

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

VENDOR INTEGRATION QUESTIONS. Questions for vendor integration include topics of security, user authentication, data, and architecture. 1 Page (20-696)

VENDOR SECURITY ASSESSMENT. This questionnaire is about secure coding, incident response, confidentiality, and other aspects of vendor security. 2 Pages (20-683)

SECURITY QUESTIONNAIRE. Designed using the NIST guide, this questionnaire will help determine the level of risk and organization will incur using the provider in question. 32 Pages (20-584)

SECURITY STANDARDS WORDING. This describes wording for information security requirements guidelines to be used for bids and RFP documents. 2 Pages (20-542)

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)

INFORMATION SECURITY REQUIREMENTS AGREEMENT. This ISR is an exhibit to the Master Services Agreement effective under which provider may be engaged from time to time to provide services. 5 Pages (20-538)

ENDPOINT SECURITY TOOL COMPARISON. An overview of one member organization's comparison of several popular "heuristic" behavioral-based endpoint security products including Carbon Black, Cylance, Darktrace, and CrowdStrike. 3 Pages (20-220)

REQUIRED SECURITY DOCUMENTATION. This table provides an example of required documentation regarding the infrastructure, application code, and network topology. 4 Pages (20-130)

DOCUMENTATION & INDIVIDUAL SECURITY EVALUATION. The Evaluator will rate how well the Proposer's solution overall satisfies the company's requirements, as well as its overall suitability for the company.
34 Pages (20-129)

SECURITY CONSULTANT REQUEST. Various security tasks such as vulnerability assessment, penetration testing, awareness training, and incident response will need to be performed by the security consultant.
5 Pages (20-106)

EVENTS MANAGEMENT SUITE. This suite is a scorecard and pricing matrix for events management vendors.
2 Pages (20-096)

VENDOR SECURITY ASSESSMENT. This Application Security Review (ASR) questionnaire enables organizations to assess security compliance and serves as a prerequisite before approval of purchase or use of applications. 17 Pages (50-264)

VENDOR SECURITY CHECKLIST. This worksheet provides questions to inquire of prospective vendors to ensure security. 3 Pages (50-192)