Toolkit

The Vendor-Free IT Community.

NETWORK MANAGEMENT & COMMUNICATIONS

These NOREX Member-contributed documents include communication, network, and systems plans, email, record retention, RFP, discussion transcripts, polls, social media, video, and questionnaires. | TK005

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

Acceptable Use

ACCEPTABLE USE POLICY. This policy establishes guidelines and responsibilities for the acceptable use of company information, technology assets, and resources. 4 Pages (20-1063)

IT GENERAL ACCEPTABLE USE POLICY. This overarching policy provides a general outline of how corporate or personal IT assets are being used to carry out company business. 4 Pages (20-1043)

ACCEPTABLE USE POLICY. The rules for acceptable use of computer equipment are in place to protect the person and the company from exposure to risks such as virus attacks. 4 Pages (20-1034)

IT SECURITY ACCEPTABLE USE. This policy manages IT resource exposure, communicates resource protection responsibility, and increases information security awareness. 5 Pages (20-1024)

ACCEPTABLE USE POLICY. Acceptable uses of computer equipment, systems, and software are provided here. Appropriate use can prevent exposure to risks including cyberattacks, data breaches, and potential legal issues. 7 Pages (20-874)

ACCEPTABLE USE POLICY. This policy outlines the acceptable use of computer equipment. 4 Pages (20-766)

COMPUTER SYSTEMS AND INTERNET USE POLICY. Established here is a framework for security and data integrity, outlining the acceptable use of computer equipment. 6 Pages (20-752)

TECHNOLOGY USE AGREEMENT. This agreement outlines the underlying principles and rules that govern the use of company information and technology. 2 Pages (20-705)

ACCEPTABLE USE POLICY. This policy sets forth guidance for the appropriate and acceptable use of company IT resources and information. 10 Pages (20-673)

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)

ELECTRONIC COMMUNICATION ACCEPTABLE USE POLICY. The topics of use, fraud, ownership, data collection, hate speech, and more are covered in this policy. 2 Pages (20-574)

ACCEPTABLE USE POLICY. This policy provides authorized users with standards for the acceptable and unacceptable use of company information technology. 4 Pages (20-482)

iPAD LOAN & USE AGREEMENT. The terms & conditions of a loaned equipment program to allow for the temporary use of equipment and computers are outlined. 4 Pages (20-409)

ACCEPTABLE USE POLICY. The purpose of this policy is to define appropriate and inappropriate use of company information assets. 7 Pages (20-322)

ACCEPTABLE USE ANNUAL CONTRACT. This agreement is about the acceptable use and confidentiality of company Information Technology assets, computers, networks, systems, and data. 2 Pages (20-318)

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

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)

Access Management

THIRD-PARTY ACCESS POLICY. This policy establishes the rules governing access to information systems, information, and computer or server room by parties such as vendors, contractors, consultants, security, etc. 5 Pages (20-924)

PHYSICAL ACCESS PROCEDURE. This document defines a procedure for who is allowed physical access to the data center and other facilities that house information systems. 2 Pages (20-923)

REMOTE ACCESS POLICY. This policy defines standards and restrictions for connecting to internal networks from external hosts via remote access technology. 3 Pages (20-921)

REMOTE ACCESS REQUEST. This form is for requesting remote access to company resources, such as network equipment. 2 Pages (20-916)

IT FACILITY ACCESS. Described is a procedure for accessing the main office company data center and network closets. 3 Pages (20-870)

REMOTE ACCESS POLICY. This policy defines the requirements necessary to remotely connect staff to the network. 3 Pages (20-826)

THIRD PARTY LIMITED ACCESS AGREEMENT. This Agreement outlines specific responsibilities that relate to vendor access to any company data that may be stored within software or on the server. 5 (20-760)

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)

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)

NETWORK ACCOUNT ACCESS FORM. In order to gain access to various levels of network departments, workstations, etc., this form should be collected. 1 Page (20-601)

ERP & INFORMATION ACCESS REQUEST FORM. The following is an access request form suitable for various security levels and information & ERP groups. 1 Page (20-600)

WINDOWS APPLICATIONS ACCESS FORM. This form provides basic information for and about persons who wish to attain access to Windows applications on the corporate network. 1 Page (20-599)

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)

ROLE BASED ACCESS CONTROL BASICS. Incorporating a Role Based Access Control (RBAC) practice into your enterprise program is the best way to handle access rights. 3 Pages (20-592)

REMOTE ACCESS JUSTIFICATION. Remote access creates an added risk to the network and computer systems. This form helps justify which employees require access and why. 1 Page (20-566)

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

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)

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)

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)

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)

Communications

WIRELESS COMMUNICATION POLICY. This policy establishes the criteria and process for the acquisition, assignment, and management of agency-owned cell phones and other wireless communication devices. 6 Pages (20-720)

VOALTE TELECOMMUNICATIONS. The use of the Voalte platform for voice, alarm, and text communications in a hospital or healthcare environment is explored in this policy. 4 Pages (20-674)

INTERNET & ELECTRONIC COMMUNICATION POLICY. This guide will give examples of proper usage and expectations for communication and messaging services and equipment. 9 Pages (20-560)

PERSONAL USE OF COMPANY COMMUNICATIONS. Company communication systems should be used only for company business or for limited incidental personal use as described in the guidelines. 2 Pages (20-479)

APPROPRIATE USE OF ELECTRONIC COMMUNICATION. Electronic mail, data, and system activity logs, including the Internet, are subject to audit and review. The appropriate use of these systems is detailed below. 5 Pages (20-320)

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

SKYPE FOR BUSINESS USE GUIDELINES. This document outlines best practices and guidance for using Skype for Business. 3 Pages (20-208)

DEVELOPING A COMMUNICATION PROGRAM. A communication plan introduces the concept of a communication program and how to develop the strategy, communication campaign definition. 20 Pages (20-197)

COMMUNICATION PLAN & MATRIX. This plan template and matrix outline deliverables, audience, and other components of communication. 4 Pages (20-196)

COMMUNICATION MANAGEMENT GUIDELINES. This is a guide through communication planning and information distribution. 7 Pages (20-195)

COMMUNICATION MEDIA COMPARISON. Several modes of company communication are compared in this document. 3 Pages (20-194)

PROJECT COMMUNICATIONS PLAN. The purpose of this document is to outline the communications that will be done throughout the project's duration. 7 Pages (20-193)

COMMUNICATION PLAN APPENDICES. This document includes several important components of a communication plan, such as agenda, minutes, event schedule, and action items. 18 Pages (20-192)

PROGRAM COMMUNICATION PLAN. This plan provides an overall framework for managing and coordinating the wide variety of communication that will directly or indirectly take place as part of the program. 10 Pages (20-191)

CIO COMMUNICATION PLAN. This general plan outlines methods of communication as well as their timeline. 4 Pages (20-014)

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)

ENTERPRISE ARCHITECTURE TRANSCRIPT. NOREX Members discussed key areas of opportunity for EA, how EA addresses internal vs external business capabilities, EA's role to contribute to current and future business financial performance, tracking metrics and measuring performance, citizen development, and advertising EA specific services across the organization. 24 Pages (NV2387)

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)

VIRTUAL COLLABORATION & BUILDING CULTURE: WORK-FROM-HOME BEST PRACTICES TRANSCRIPT. NOREX Members discussed reconciling and standardizing a hybrid workforce, combating organization culture loss, maintaining productivity, security, connectivity issues, equipment reimbursement, and scheduling and hoteling solutions. 22 Pages (NV2373)

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)

ENTERPRISE STORAGE SOLUTIONS TRANSCRIPT. Member organizations discuss a variety of enterprise storage technology, trends, vendor solutions, and more during this March 2021 WebForum. Several polls are included. 24 Pages (NV2362)

TELECOM / VOIP / TEAMS PHONE SYSTEMS TRANSCRIPT. A great March, 2021 discussion on telecom trends. Strategies and experiences moving to Teams (and others) for voice; softphones comparison; VoIP enhancements; and more. This transcript includes several polls and a lively chat session. 32 Pages (NV2361)

VDI AND DESKTOP AS A SERVICE (DaaS) TRANSCRIPT. Members discuss their adoption to both VDI and DaaS environments during this February, 2021 WebForum. This discussion includes a detailed look at one members journey, several polls, and a lively chat. 18 Pages (NV2360)

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)

ENDPOINT SECURITY TRANSCRIPT. NOREX members discussed different Endpoint Protection and Endpoint Detection & Response tools and strategies during this September, 2020 WebForum. Significant takeaways 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)

HYBRID AND MULTI-CLOUD ENVIRONMENTS TRANSCRIPT. Members compare notes and experiences with both Multi-Cloud and Hybrid Cloud environments during this August, 2020 WebForum. Use cases for different cloud providers, tools, and strategies are discussed. 17 Pages (NV2338)

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

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

REPLACING SKYPE FOR TEAMS / TEAMS TELEPHONY ISSUES TRANSCRIPT. NOREX Member organizations weigh in on the status of a move to Teams telephony from either an on-prem or cloud Skype for Business solution and / or other vendor systems during this July 2020 session. 22 Pages (NV2330)

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)

SERVICENOW TRANSCRIPT. NOREX Members currently using or evaluating ServiceNow discuss justification, ROI, implementation, SLA best practice, and specific functionality during this June 2020 session. 20 Pages (NV2327)

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)

MICROSOFT TEAMS GOVERNANCE TRANSCRIPT. NOREX Members and guests share their experience, questions, and ideas on Microsoft Teams. This WebForum explored issues including best practices, migration, retention, managing groups, naming conventions, guest access, add-ins, and creation and archiving of teams. 49 Pages (NV2322)

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)

VDI TRANSCRIPT. NOREX Members discuss the selection, implementation and operation of various Virtual Desktop Infrastructure platforms during this February 2020 WebForum. 16 Pages (NV2306)

SD-WAN TRANSCRIPT. NOREX Members discuss the reasons they have moved forward or are considering the benefits of SD-WAN technologies during this January 2020 WebForum. 14 Pages (NV2304)

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)

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)

HELP DESK / SERVICE DESK TRANSCRIPT. NOREX Members discuss Help Desk / Service Desk procedures and recommended tracking tools during this November 2019 WebForum. 14 Pages (NV2296)

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)

MICROSOFT TEAM TRANSCRIPT. Microsoft Teams is gaining momentum for several NOREX organizations. While many are in the beginning stages, addressing Teams governance, retention concerns, managing access, general engagement, and more are discussed during this September, 2019 WebForum. 22 Pages (NV2287)

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)

TELECOM / MOBILE / VOIP ISSUES TRANSCRIPT. NOREX members discuss Mobile Device Management, VoIP solutions and telecom issues during this August 2019 session. 15 Pages (NV2284)

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)

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)

WEB CONTENT MANAGEMENT TRANSCRIPT. NOREX members had good discussion during this May 2019 WebForum. Content includes the selection process, tools used, best practices, and much more. 12 Pages (NV2271)

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)

DIGITAL ASSET MANAGEMENT TRANSCRIPT. NOREX members discuss digital asset management strategies, roadmaps and tools during this February 2019 session. 11 Pages (NV2257)

CLOUD-BASED STORAGE TRANSCRIPT. NOREX members discuss the pros and cons of moving from on-prem to cloud-based storage during this January 2019 session. 16 Pages (NV2254)

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: 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 licensing program during this October 2020 WebForum. 19 Pages (GSP100)

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)

Email

EMAIL MANAGEMENT & RETENTION. This policy covers the review, retention, and destruction of email and email attachments received or sent by company representatives. 5 Pages (20-873)

EMAIL RETENTION POLICY. Storage and retention requirements for company email are described here, as well as requirements for public record email retention. 3 Pages (20-703)

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

EMAIL RETENTION POLICY. This policy advances the best practices in capturing, managing, and retaining electronic messages. 5 Pages (20-641)

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)

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)

E-MAIL USE & STORAGE POLICY. The rules for the use and management of company systems for sending, receiving or storing of e-mail and electronic faxes (e-Fax) are established. 6 Pages (20-403)

E-MAIL & DATA RETENTION. The following is an e-mail retention policy and a general data retention policy overview. 3 Pages (20-355)

ELECTRONIC MEDIA POLICY. Appropriate use of eMedia to communicate information electronically is defined. 7 Pages (20-153)

ELECTRONIC MAIL USE & GUIDELINES. These policy statements fall into five categories: privacy, acceptable use, security, retention, and monitoring/access. 7 Pages (20-071)

E-MAIL USE & RETENTION. This policy addresses privacy, security, and legal issues related to use of company e-mail services. 5 Pages (20-064)

E-MAIL SERVICES / OFFICE SUITE EVALUATION. Following is a comparison of the functional requirements and cost summary of Web-Based Office Suite (WBOS) such as Google Apps or Office 365. 16 Pages (20-061)

Network, Systems Plans

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

NETWORK CONNECTION STANDARDS. Separating the network into various segments (VLAN) ensures that systems can easily communicate with each other and exchange data. One such separation is demonstrated here. 6 Pages (20-768)

COMPUTER MONITORING PROCEDURE. Normal computing resource operation and maintenance requires backup and caching of data & communications, logging activity, monitoring general usage patterns, and other activities necessary for providing service. 3 Pages (20-763)

DNS NAMING STANDARDS. Naming standards for internal Domain Name Service (DNS) websites are exemplified here. 2 Pages (20-700)

LAN SWITCH UPGRADE. This presentation offers recommendations and data regarding a Local Area Network upgrade. It compares the use of Avaya, Aruba, and Cisco systems. 19 Pages (20-686)

SYSTEM PORTFOLIO DATABASE FIELD LIST. This spreadsheet provides a format for recording database fields with system detail, cost/resources, and user group & function. 9 Pages (20-330)

SYSTEM PORTFOLIO DEFINITIONS. Defined below is a system portfolio including application types, category types, availability, and software type. 2 Pages (20-329)

SYSTEM AVAILABILITY OBJECTIVES. System availability is tracked for key components of the infrastructure and for critical applications. The expected availabilities for infrastructure, enterprise software, web presence, application software, and council remote access are defined. 3 Pages (20-310)

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)

NETWORK WIRING CLOSETS. These are general requirements and planning points for network wiring closets. 1 Page (20-105)

MONITORING SOLUTION SELECTION. Following is a checklist of functionality, troubleshooting, and interactive services to help make a decision on a monitoring solution. 1 Page (20-048)

Patch Management

PATCHING TOOL VENDOR MATRIX. This weighted scoring template compares several patching tool vendors by service and performance. 2 Pages (20-1056)

IT SYSTEM MAINTENANCE. This is a procedure for maintaining activities for server, enterprise storage, and infrastructure systems. 5 Pages (20-872)

EMERGENCY PATCHING STEPS. This document shows the out-of-band patching steps for deploying emergency patching via Symantec Client Management Suite (Altiris). 6 Pages (20-843)

PATCHING PROCESS. This is an example of a patching schedule broken into two main patch weeks, with a third week available if needed. 1 Page (20-737)

PATCH CABLE ORDER FORM. This order form is for ordering cable for the equipment room, telecom closet, and data center. 1 Page (20-548)

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)

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)

Policies, Procedures and Guidelines

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

IT INSTALLATION STANDARDS. This document serves as the basis to provide an easy to support, reliable, and consistent networking baseline consisting of cabling, component, and installation standards. 11 Pages (20-771)

WI-FI BASIC STANDARDS. More devices are being connected to corporate networks that utilize wireless connectivity. This document provides company standards. 5 Pages (20-769)

COMPUTER SYSTEMS USE AGREEMENT. Computer systems and internet use are outlined, followed by a user agreement. 4 Pages (20-753)

COMPUTER SYSTEMS AND INTERNET USE POLICY. Established here is a framework for security and data integrity, outlining the acceptable use of computer equipment. 6 Pages (20-752)

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)

DATA BACKUP POLICY. This policy sets a consistent standard concerning the appropriate stewardship of digital data with respect to company requirements as well as obligations to state and federal laws. 9 Pages (20-559)

TECHNOLOGY USE POLICY. This policy establishes standards for the maintenance & protection of information systems infrastructure, including all equipment, software, and systems. 8 Pages (20-558)

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)

END USER COMPUTING & PRINTER POLICY. End user provisioning, asset security, roles, and responsibilities are defined in this policy. 5 Pages (20-510)

IT USE POLICY. This policy governs the security, availability, and acceptable use of computing equipment, data & network access, and general-purpose technology. 12 Pages (20-485)

INTERNET & INTRANET USE POLICY. This policy covers employee access to Internet sites, blogs, and any web- based publications as well as company Intranet sites. 2 Pages (20-478)

LOGGING RECORDER POLICY. Especially useful for those who use dispatching, this document is designed to provide for a secure and uniform method of recording and storing recorded media. 2 Pages (20-396)

TECHNOLOGY USE POLICY. This document sets forth general principles on use of technology and services within the company. 6 Pages (20-368)

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)

EMPLOYEE IT SYSTEMS POLICY. IT systems are managed in a manner that maintains the integrity and security of records, as well as the confidentiality of sensitive information and data. 4 Pages (20-289)

INFORMATION SYSTEMS USE. This policy describes appropriate use of company information systems and defines prohibited acts. 5 Pages (20-052)

ELECTRONIC SIGNATURE POLICY. This policy provides for the legally recognized use of an electronic signature (e-Signature) to replace a written signature in some company business activities. 4 Pages (20-051)

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)

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: BACKUP/ STORAGE. This Backup and Storage Tools and Solutions poll resulted in 51 products being rated. One hundred and thirty members responded. 6 Pages (NR004)

MEMBER VENDOR RATINGS: PATCH MANAGEMENT. This Patch Management Tools and Solutions poll resulted in 24 products being rated. One hundred and thirty members responded. 2 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)

MEMBER VENDOR RATINGS: HELP DESK. This Help Desk Tools and Solutions poll resulted in 56 products being rated. One hundred and thirty members responded. 8 Pages (NR001)

QUICK POLL RESULTS: TECHNOLOGY AND 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)

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)

Records Management

RECORD RETENTION POLICY. The goals of this Policy are to retain important records for reference and future use and delete or destroy records that are no longer necessary. 18 Pages (20-1052)

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)

RECORDING, INDEXING, & IMAGING SOW. A company is looking for a complete turnkey solution to include all software, hosting, equipment, archival microfilm creation, and support. 25 Pages (20-611)

RECORDS & INDEXING EQUIPMENT LIST. Computer systems and workstation equipment for scanning, printing, cashier stations and research are listed here. 3 Pages (20-608)

RECORD RETENTION, STORAGE, & DESTRUCTION. A process for management of records, their retention, storage, and destruction is designated in this document. 25 Pages (20-159)

SHAREPOINT DOCUMENT & RECORDS MANAGEMENT. This document outlines foundational & advanced document/records management and eDiscovery with SharePoint. 3 Pages (20-006)

Reporting

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

REPORT REQUIREMENTS SPECIFICATION TYPE 1. This form helps to determine what required elements of your reports need to be and how they are to be organized. 5 Pages (20-621)

REPORT REQUIREMENTS TABLE. A report table captures the detailed level requirements for a single report. The following is an example of this type of table. 4 Pages (20-620)

EXAMPLE REPORTING REQUIREMENTS. This is an example of the types of required elements that make up a functional report. 3 Pages (20-619)

REQUIREMENT GATHERING QUESTIONNAIRE. This series of questions provide information about required elements of reports, from frequency and access to parameters and reporting metrics. 2 Pages (20-618)

REPORT DEFINITION WORKSHEET. Report owner, designer, audience, and report details are described in this worksheet. 3 Pages (20-617)

RFP & Contracts

RFP: CLOUD COMPUTING PROVISIONING SERVICES. This document solicits proposals for a cloud-based solution for optimal architecture, security, performance, and strategic vision. 17 Pages (20-881)

RFP: INTERNET SERVICES. This RFP will assist in selecting a qualified service provider for one or more internet services at one or multiple locations. 16 Pages (20-854)

RFP: VOICE SYSTEM SOLUTION. An organization seeks proposals to provide a replacement of their current PBX phone system and centralized voice mail system. 40 Pages (20-734)

RFQ: IT INFRASTRUCTURE ASSESSMENT. An IT Senior Leadership team is requesting quotes for an overall IT Infrastructure Assessment with a focus on operational excellence and high availability of Tier 1 systems. 3 Pages (20-644)

RFP: RECORDING, INDEXING, & IMAGING SYSTEM. This office is seeking the latest technological advances and hardware, including recording/cashiering with integrated scanning and indexing capabilities, e-recording, verification, bookkeeping/treasury functionality, hardware, implementation services, annual maintenance, production support, and microfilm creation/storage. 10 Pages (20-610)

RFP: COMPUTER HARDWARE, SOFTWARE & SERVICE. An organization seeks a single vendor solution for computer hardware (computers, servers, and related hardware), software, and Microsoft Volume License Purchase Program and related services. 30 (20-463)

RFP: COMPUTERS & PERIPHERALS. This RFP is seeking computers and/or related computer peripherals or components with the best price/performance ratio and the ability to provide service and support for said equipment. 16 Pages (20-462)

RFP: COMPUTER LEASE/PURCHASE. This RFP is mainly focused on the service aspects of hardware deployment and technology leasing for a university setting. 8 Pages (20-461)

RFP: CAD/RECORDS MANAGEMENT. Following is a proposal request for a Computer Aided Dispatch (CAD) and Records Management System as well as its implementation and maintenance. 122 Pages (20-446)

RFP: WIRELESS ACCESS POINT. Proposals are requested for installation of new wireless access point equipment such as Xirrus Wi-Fi or equivalent. 6 Pages (20-380)

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)

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)

RFP: INTERNET SERVICES. This request solicits proposals from qualified firms for telecommunications / data communications to provide Internet connectivity. 12 Pages (20-077)

Scorecards & Questionnaires

VENDOR SCORECARD QUESTIONS. Initial questions and electronic requirements are covered in this vendor scorecard for HR & Payroll solutions. 13 Pages (20-716)

SYSTEM SCORECARD & COMPARISON. This worksheet shows a way to compare and score financial tech systems. 5 Pages (20-677)

DIGITAL SIGNAGE SOLUTIONS. Solutions for digital signage and wireless display are listed, with links to each website to explore your options. 3 Pages (20-507)

WEB HOSTING QUESTIONNAIRE. This document gathers detailed customer requirements for proposed web hosting projects. 4 Pages (20-411)

TELEPHONE SCORECARD TEMPLATE. This scorecard rates everything from consoles, voice mail, and calendaring to conference calling and IVR recording. 21 Pages (20-151)

PHONE SYSTEM POC. This proof of concept discusses replacement of an aging phone system with Avaya PBX or hosted system. 12 Pages (20-074)

VENDOR SCORECARD. Here is an example of a vendor scorecard, weighing services, quality, cost, etc. 4 Pages (20-040)

Server

SERVER ROOM ACCESS & STORAGE COMPLIANCE. The server room provides enhanced reliability and security for IT components. This procedure describes access and storage limitations. 1 Page (20-765)

SERVER BUILD REQUEST TEMPLATE. The following process can be followed when it becomes necessary to request new servers. 4 Pages (20-738)

SERVER LIST BY TIER. This worksheet illustrates a method of listing servers, function, operating system, and other details. 4 Pages (20-680)

Social Media

SOCIAL MEDIA USE POLICY. This policy establishes guidelines for the use of social media. 3 Pages (20-632)

SOCIAL MEDIA POLICY. This policy is intended to assist employees in making appropriate decisions about work-related blogging and social media interaction. 9 Pages (20-381)

SOCIAL MEDIA GUIDELINES. The following guidelines provide policy on the use of social media in an educational workplace setting, and how it could be linked to your personal online presence. 6 Pages (20-376)

SOCIAL MEDIA GUIDELINES. Originally prepared for an organization in education, this document includes discussion on professional social media use as well as site monitoring. 4 Pages (20-263)

SOCIAL MEDIA POLICY TRAINING. Tips on how to share and engage in social media, demographics, and working with agency (or company) accounts. 21 Pages (20-137)

Video

SETTING UP A FREE ZOOM ACCOUNT. Instructions for signing up for a free videoconferencing account through Zoom including tips for activation. 7 Pages (20-1076)

REMOTE VIDEOCONFERENCE BEST PRACTICES. Tips for participants and for meeting organizers while videoconferencing from remote workstations at home. 1 Page (20-896)

VIDEO CONFERENCING TROUBLESHOOTING. With staff working remotely, video conference sessions are becoming a more common occurrence. Because each person's internet access at home can be different and their experience with video conferencing varies, this document will be helpful for troubleshooting guidance and tips. 2 Pages (20-892)

VIDEO MEETINGS BEST PRACTICES. This document includes a few simple camera and audio tips to make your video conferencing experience successful. Specific tips on Google Hangouts are included. 1 Page (20-891)

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)

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)

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)

INMATE VIDEO VISITATION. The purchase, installation, and maintenance of an Inmate Video Visitation System to provide remote video visitation for the public, attorneys, and officials are explored in this presentation. 11 Pages (20-214)

CONFERENCE CALLING WITH BLUEJEANS. These are tips on using BlueJeans, a video conferencing service that connects participants across a wide range of devices and conferencing platforms. 10 Pages (20-025)