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

TO REQUEST A DOCUMENT FROM THIS TOOLKIT, NOTE THE TITLE / NUMBER AND ADD THEM TO THE COMMENTS AREA ON THE REQUEST FORM HERE.

Acceptable Use

GENERAL IT ACCEPTABLE USE POLICY This overarching policy is designed to provide a general outline of how corporate or personal IT assets are being used to carry out company business. 4 Pages (20-1293)

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 Rules governing third-party access to information systems, server rooms, third-party responsibilities, and information protection make up this policy. 5 Pages (20-1296)

REMOTE ACCESS POLICY This policy defines standards and restrictions for connecting to internal network(s) from external hosts via remote access technology and usage via third-party wireless internet service providers. 4 Pages (20-1295)

PRIVILEGED ACCESS MANAGEMENT POLICY This access standard has been developed to reduce risk to IT resources and systems. 5 Pages (20-1137)

WEBSITE ACCESSIBILITY STATEMENT This standard provides information on disclosing efforts made to increase accessibility to a public website in accordance with the ADA and other regulations. 3 Pages (20-1135)

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 Pages (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)

IDENTITY & ACCESS MANAGEMENT POLICY This policy applies to management of user accounts and access to shared information within a database, application, or shared file space. 12 Pages (50-417)

USER PASSPHRASE STANDARD The creation of passphrases, their protection, and the frequency of change are established in this policy. 3 Pages (50-416)

Communications

ELECTRONIC MONITORING POLICY This policy outlines the tools and resources employees use that can be monitored for business reasons. 2 Pages (20-1216)

ELECTRONIC MONITORING POLICY This policy establishes guidelines for company practices and procedures related to the electronic monitoring of employees. 2 Pages (20-1215)

MS TEAMS PHONE SYSTEM PLAN The following is a design plan for implementation of Microsoft Teams Online with Direct Routing and Cloud Voicemail. 28 Pages (20-1129)

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)

PROJECT PLAN AND MATRIX This worksheet includes a project planning template and tables for tracking products at different locations. 5 Pages (50-395)

Email

INTERNET AND EMAIL POLICY All internet use and email transmission is monitored by the company, as described in this policy. 4 Pages (20-1292)

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

GUEST AND EMPLOYEE WIRELESS NETWORK POLICY The standards, procedures, and restrictions for connecting to and using guest and employee wireless networks are outlined. 4 Pages (20-1294)

NETWORK ARCHITECTURE TEMPLATE This diagram outlines a typical network architecture system. 1 Page (20-1278)

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

VULNERABILITY MANAGEMENT This document explores vulnerability identification, evaluation, reporting, timeline, and response. 3 Pages (20-1155)

PATCHING BEST PRACTICE SUGGESTIONS This policy suggests automating patching in order to expedite the process. 1 Page (20-1154)

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

ANTIVIRUS POLICY This policy provides instructions on measures to help achieve effective virus detection and prevention. 4 Pages (20-1297)

TECHNOLOGY ACQUISITION WITH OPERATIONS SUPPORT This procedure describes maintaining compliance with minimum standards for connectivity to the network. 2 Pages (20-1177)

BEST PRACTICES SECURITY REVIEW This overview of network security includes acceptable use, information privacy and classification, network access, and more. 2 Pages (20-1176)

ITS POLICY HANDBOOK This policy includes a variety of IT policies such as security, configuration & systems management, access control, and communications. 109 Pages (20-1116)

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)

Records Management

RECORDS RETENTION PROGRAM This is an example of a government organization's policy and procedure on retention of email and other company records. 12 Pages (20-1190)

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: PHONE SYSTEM UPGRADE This example RFP invites proposals to provide phone system upgrade and replacement. 19 Pages (20-1108)

WAN SERVICES QUESTIONNAIRE This group of sample questions refers to an RFP for provision of wide area network services. 2 Pages (20-1107)

RFP: WAN SERVICES An organization is seeking a comprehensive solution with an innovative, market- leading vendor of wide area network services. 19 Pages (20-1106)

RFP: TELEPHONY SERVICES This RFP helps identify and select the most appropriate business partner for telecommunications services. 10 Pages (20-1101)

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)

UC-VOICE RFP This is a sample RFP for Unified Communications Voice (UC-Voice) as a Service. 15 Pages (50-394)

Scorecards & Questionnaires

TEAMS CALLS USER SURVEY This questionnaire asks users to provide details on training, use, and satisfaction with MS Teams Calls. 3 Pages (20-1162)

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 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

FIREWALL POLICY This policy describes how the firewall will filter network traffic to mitigate risks and losses associated with security threats, while maintaining appropriate access levels. 3 Pages (20-1298)

SECURE MS SQL DATABASE This standard guides consistency in the configuration of Microsoft SQL servers, including a secure database configuration checklist. 7 Pages (20-1134)

SECURE WINDOWS SERVER CONFIGURATION This standard provides guidance for a secure Windows server configuration covering any device running on a Microsoft Windows operating system. 5 Pages (20-1130)

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

HIPAA AND SOCIAL MEDIA STANDARDS These standards provide a guideline for reducing the risk of privacy violations related to social media. 1 Page (20-1238)

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)

VIDEOCONFERENCING 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)

Transcripts & Polls

BANKING / FINANCIAL INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed compliance issues; regulatory trends; onboarding / offboarding software; AI usage; AI / ML for enhanced customer service; Cloud usage; IT staffing trends; remote work trends; and the impact of AI on IT careers. 15 Pages (NV2503)

DATA ENCRYPTION TRANSCRIPT NOREX Members discussed data encryption pros and cons; implementations; encouraging the use of data encryption in the enterprise; standards; file sharing considerations; encryption in a hyperconverged environment; BitLocker recovery; tools; emerging technologies; encryption issues in China; and USB encryption. 14 Pages (NV2501)

PROJECT MANAGEMENT TRANSCRIPT NOREX Members discussed software tools; Azure DevOps; tools for IT vs the enterprise; MS Project; project queue visualization; scoring models; use of AI; MS Copilot; automating with Power BI; workflow approval; Teams for projects; success measurements; decommissioning projects; and lessons learned. 20 Pages (NV2499)

MICROSOFT INTUNE TRANSCRIPT NOREX Members discussed reasons for implementing Intune; Intune for smaller organizations; features; key steps for deployment; group policies; distributed resources sharing the same environment; and reporting. 19 Pages (NV2497)

MANAGING TECHNICAL DEBT TRANSCRIPT NOREX Members discussed the definition of technical debt; problems that occur; cleaning up a ServiceNow database; upper-level support; cyber attack risks; strategies to remediate technical debt; budget considerations; security risks; project delivery considerations; and Cloud vs on-prem technical debt. 18 Pages (NV2496)

CONSTRUCTION INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed security concerns for 2024; phishing; shadow IT; AI solutions; multi-Cloud for AI offerings; ERP solutions; utilizing P6 in the Cloud; collaboration tools for corporate IT and project engineers; internet connectivity for remote sites; and diversity tracking tools. 24 Pages (NV2493)

RANSOMWARE TRANSCRIPT NOREX Members discussed lessons learned; paying or not paying the ransom; ethical and legal considerations regarding payment; engaging outside assistance; ransomware plan vs cybersecurity plan, immutable backup; early detection; reporting an attack; security and vulnerability assessments; and cybersecurity insurance considerations. 16 Pages (NV2488)

TRANSPORTATION INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed cybersecurity practices and tools; automating cybersecurity processes; user training videos; Azure Sentinel; securing personal messenger apps; WhatsApp security considerations; vendor flow; deploying MFA for all types of access; applying security certificates; black box device security; predictive ETA tools; and capturing real-time vehicle data. 14 Pages (NV2486)

IDENTITY & ACCESS MANAGEMENT TRANSCRIPT NOREX Members discussed the maturity of IAM in the organization; identity governance and roles; Entra; systems to prioritize when implementing IAM solution; tools in use; relying solely on Microsoft products; first-time login credentials; authentication options for the young and disabled; and biometrics and digital authentication methods. 17 Pages (NV2485)

SD-WAN TRANSCRIPT NOREX Members discussed SD-WAN pros and cons; deployment; the complexity of SD-WAN; public vs private internet connections; backup strategies; cost considerations; quality-of-service experiences; firewall positioning; P2P traffic performance; VPN connections; vendor selection; Fortinet usage; Cisco vs Meraki; utilizing multiple vendor solutions; Palo Alto; managed services options; SASE; WAN acceleration; and Always On VPN. 19 Pages (NV2483)

MANUFACTURING INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed aligning IT with manufacturing processes; the “walkabout” model; implementing an enterprise-wide approach; network segmentation strategies; patching floor systems; Manufacturing Execution Systems (MES); ERP integration with manufacturing processes; authentication for frontline workers; Microsoft Dynamics; and dedicated operational technology. 18 Pages (NV2482)

ENDPOINT DETECTION & RESPONSE TRANSCRIPT NOREX Members discussed the definitions of EDR, MDR, XDR, SOAR, and SIEM; managing SOAR and SIEM systems; endpoint solutions and tools in use; Huntress.io; Windows Defender; EDR and the remote work environment; false positives; and SOC or managed SIEM products. 14 Pages (NV2480)

MERGERS & ACQUISITIONS TRANSCRIPT NOREX Members discussed merger and acquisition experiences and recommendations; acquiring executive consideration for technical issues; M&A planning; managing due diligence; identity federation; migrating Active Directory and Microsoft Forms; platform and cross-platform migration tools; ERP migration; domain access; management software / discovery tools to inventory IT asset inventories; and enterprise reporting platforms. 16 Pages (NV2473)

PRIVACY LAWS TRANSCRIPT NOREX Members discussed privacy law compliance; departments best suited to manage privacy; sources consulted to measure compliance against; developing and keeping current a Record of Processing Activities (ROPA); Privacy Impact Assessments (PIA) tools; NIST CSF core functions; Chief Privacy Officer or Chief Compliance Officer; audit frequency of IT tools to ensure privacy law compliance; leveraging internal audits to evaluate privacy programs; and US federal legislation on privacy laws. 13 Pages (NV2471)

ARTIFICIAL INTELLIGENCE / MACHINE LEARNING / ChatGPT TRANSCRIPT NOREX Members discussed how AI is used for critical thinking; use cases; training internal models – LLM; tracking the validity of AI info and privacy concerns; real world use cases; training users; policies for use; limiting personal logins to ChatGPT; deciding when to use; tracking users’ usage of AI / ChatGPT; chatbots and OpenChatKit; and copyright protections in AI. 20 Pages (NV2470)

MFA & IDENTITY ACCESS MANAGEMENT FOR ADMINISTRATORS TRANSCRIPT NOREX Members discussed the definitions of MFA, IAM, and PAM; cyber insurance requirements; MFA tools; MFA usage trends; enforcing MFA with M365; MFA for non-admins; MFA for non-service accounts; threat detection and response; automated detection tools; passwordless authentication; phishing resistant MFA; and password vault usage. 21 Pages (NV2468)

ANTIVIRUS & FIREWALLS TRANSCRIPT NOREX Members discussed antivirus and firewall vendors; Mimecast and Artic Wolf; FortiGate; Azure site recovery; handling endpoint protection and leveraging both an endpoint protection platform and endpoint detection and response solution; host-based firewalls; firewalls in HA mode; how SDN networking usage affects firewall controls; methods used in exercising granular control over traffic exceptions; Azure firewalls; moving from SonicWall to FortiGate; and alternatives for Palo Alto firewalls, MS Defender antivirus, and Proofpoint email filtering. 17 Pages (NV2466)

ENERGY / UTILITY INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed budget trends; technology and innovation challenges; effective collaboration and communication between IT and OT; Cloud solutions for CIP data / workloads and auditing concerns; SaaS and Cloud options for major applications; and ServiceNow on-prem and other tools. 15 Pages (NV2465)

CONFERENCE ROOM TECHNOLOGY SOLUTIONS TRANSCRIPT NOREX Members discussed conference room monitoring and management strategies; staff dedicated to conference room management and troubleshooting; training capable users; tool experiences and recommendations; cost of conference room technology solutions; projectors vs TVs; moving away from complex-type rooms to Microsoft Teams rooms; Microsoft licensing; camera options; using Teams with non-Teams meetings; hybrid solutions; accommodating classroom meetings; microphone considerations; and large occupancy rooms. 25 Pages (NV2464)

GOVERNMENT: CYBERSECURITY TRANSCRIPT NOREX Members discussed significant changes to the cybersecurity program considering the current threat landscape; optimizing the organizational structure; cybersecurity priorities for leadership; AI considerations; accommodating business needs while maintaining effective security; recommended cybersecurity tools; Microsoft tools utilized; G3 M365 licensing experiences; and security frameworks. 14 Pages (NV2463)

CLOUD PHONE SYSTEMS TRANSCRIPT NOREX Members discussed initial cost per user for a Cloud phone system vs VoIP system; Cloud phone providers and moving from a Cisco Unified Communication Manager (CUCM) VoIP system; Teams integration (8x8 vs RingCentral vs others); direct routing vs Cloud-hosted / managed; replacing an older on-prem Mitel system; Dialpad usage; issues with Teams; Operator Connect or direct routing integration with Teams; Vonage Premier unified communications with mobility; all-in-one VoIP / chat / video / mobile solutions for call routing workflows and SMS user requirements; devices on desktop vs softphones; Kari's Law and RAY BAUM'S Act compliance with regard to Cloud Phone Systems; and data ownership and PCI considerations. 23 Pages (NV2460)

DATA GOVERNANCE TRANSCRIPT NOREX Members discussed how data governance is defined and does it include data quality and master data; the scope of data governance (creation to deletion); who drives data governance; critical departments included in data governance; best practices and framework to launch data governance; balancing data governance with self-service reporting; tips to get the business to see the value in data governance; tactics to push business units to take ownership of data; tools used in tracking and starting a data governance committee; handling compliance and security questionnaires asking assets to be classified with a data label; social media apps on corporate cell phones; stakeholders for data-only Change Advisory Board; and integrating disparate software solutions / single product that delivers 80% for governance.
14 Pages (NV2459)

IT GOVERNANCE TRANSCRIPT NOREX Members discussed defining and initiating IT Governance; lessons learned; data governance; pain points when starting IT governance; ensuring effective governance; where IT governance sits in the organization; authority to accept or reject proposed governance policies; promoting governance as a value-add; producing policies and guidelines; governing "citizen development"; governance tools; and securing vulnerable legacy systems. 18 Pages (NV2457)

DATA ANALYTICS / BUSINESS INTELLIGENCE TRANSCRIPT NOREX Members discussed challenges with Data Analytics and Business Intelligence; dedicated teams to manage DA / BI; tooling in use; Azure Analysis and Synapse analytics; third-party connectors; Cloud vs on-prem vs hybrid environments; leveraging Cloud computing resources to improve data modeling and processing times; implementing a Master Data Management solution; Machine Learning deployments; enabling self-service capabilities; data quality; and measuring the effectiveness of DA / BI systems. 20 Pages (NV2456)

PRIVILEGED ACCESS MANAGEMENT TRANSCRIPT NOREX Members discussed responsibility for managing and maintaining privileged accounts; consolidating PAM responsibilities into a centralized program or federating them amongst different teams; implementing PAM into an IAM program; process to identify roles and entitlement taxonomy to be used by PAM; how often to review PAM in a given year; frequency of auditing role-based access management; Information Governance Administration (IGA) as an alternative or augmentation to traditional PAM systems; ensuring compliance with access policies; products and tools used to manage privileged access; PAM solutions for small organizations; password vaults; and KPI and KRI reporting. 20 Pages (NV2454)

AGILE / DEVOPS TRANSCRIPT NOREX Members discussed a framework to advance the transition from a Waterfall to Agile mentality; strategies to grow Agile maturity within an organization; moving support and product management to a Agile / Scrum-based model; best practices for managing Agile projects that impact multiple applications; rolling out a DevOps initiative; and migrating from Azure DevOps on-prem to Azure DevOps in the Cloud. 12 Pages *(*NV2452)

SD-WAN TRANSCRIPT NOREX Members discussed SD-WAN vs traditional WAN; pitfalls and costs of deploying SD-WAN; best SD-WAN solutions; replacing virtual SonicWall appliances at locations with Fortinet devices; performance SLAs in use; managing your own SD-WAN equipment vs using a managed services approach; pros / cons of using single vendor for all networks vs using a standalone SD-WAN next to the big-name network solutions; using SD-WAN to connect to Cloud service providers; using IPsec tunnels; managing multiple carriers; and using SD-WAN to provide communications for SCADA systems. 20 Pages (NV2448)

HEALTHCARE INDUSTRY IT SECURITY TRANSCRIPT NOREX Members discussed when risk outweighs an operational mandate; managing comprehensive security; successful tool and processes for centralized or almost-centralized security management; state of cybersecurity infrastructure; routine tests to measure cybersecurity readiness; managing outside access requests such as VPN connections, vendor contract workers, etc.; Cloud-hosted EMRs; responding to natural disasters or other emergencies; and best practices for recruiting and retaining talent. 14 Pages (NV2447)

NETWORK MANAGEMENT TRANSCRIPT NOREX Members discussed Network Management challenges and trends for 2023; utilizing a partner to monitor and manage infrastructure; internal Network Operations Center (NOC) and the KPIs leveraged to communicate NOC performance; network services metrics generated on the network systems and services; network performance and diagnostic products in use; utilizing a SEIM and whether it is managed internally or by a third party; Remote Syslog and iLO preferred to DRAC; best practices for network file sharing outside the organizations and maintaining consistent security for individual user OneDrive file sharing. 20 Pages (NV2445)

PATCH MANAGEMENT TRANSCRIPT NOREX Members discussed the best tools other than WSUS for patching servers and the time to report after the patch is installed; the level of automation when patching servers; automation tools for patching 3rd-party software besides SCCM; process for manually patching servers / software; enforcing or forcing workstation reboots to ensure updates and patches are applied; efficient patching and vulnerability scan frequency; VDI patching; Linux patching; Ivanti with Intune; and updating hardware drivers. 13 Pages (NV2444)

CHANGE MANAGEMENT TRANSCRIPT NOREX Members discussed frequency to allow changes; strategy used to define change windows; intake and prioritization of change requests; Change Advisory Board (CAB); change management toolsets; integrating automated configuration change technologies to catch unauthorized changes; tracking changes in SaaS, IaaS, or PaaS configurations; security review of changes; IT Change Management integration with overall company change management process; maturing Change Management / change enablement process; and change Management in DevOps, CI / CD, and Infrastructure as Code. 20 Pages (NV2439)

CONSTRUCTION INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed percentage of annual revenue spent on IT; percentage of budget allocated to IT and cybersecurity; staffing ratios; pros / cons with outsourcing support to a third party; dealing with consistent communication for “undesked” workers; internet access solutions for jobsites and remote locations; paperless onboarding with users not wanting an email address; fleet management software / services in use; Oculus VR headset and local administrator rights; asset label printers for barcodes / QR codes; structure and function of a Project Management Office for IT; and iPad programs. 19 Pages (NV2436)

ERP STRATEGIES TRANSCRIPT NOREX Members discussed managing ERP workload across the organization's teams; running ERP globally; on-prem vs Cloud-hosted, single vs multi-instance, regional support vs central support teams; running multiple unique ERPs and financial considerations; implementing Electronic Data Interchange (EDI); the value of implementing an EDI solution and ERP solution; Dynamics 365 ERP accessing ERP data through the Dataverse; Asset Management features of Dynamics F&O; implementing a WMS; migrating from EBS to another ERP system; SAP ECC to SAP S/4; and keeping inventory in sync between 3PLs and the ERP. 17 Pages (NV2435)

PASSWORD MANAGEMENT TRANSCRIPT NOREX Members discussed NIST password guidelines; verifying users for password reset without using the last four of SSN or employee ID number; critical steps to be taken before rolling out a Password Management solution; enterprise, end-user password solutions (LastPass, 1Password, Keeper, and Dashlane); user adoption of an Enterprise Password Manager; Windows Hello for Business and Beyond Identity for passwordless authentication; utilizing an MFA security thumb key; requiring two-factor or multi-factor authentication; and secure backup strategy. 21 Pages (NV2434)

MULTI-FACTOR AUTHENTICATION / SINGLE SIGN-ON TRANSCRIPT NOREX Members discussed preventing MFA fatigue; minimizing the impact to registration of the users before enabling MFA; passwordless MFA configured through Microsoft Azure by conditional access; applying MFA for service accounts; handling MFA for admins; utilizing PAM solutions and if this will be a requirement for cyber insurance; white glove configuration of new laptops; startup difficulties to retrofit SSO into the existing environment; and adopting SSO for third-party accounts that employees frequently access. 19 Pages (NV2432)

ENDPOINT DETECTION & RESPONSE TRANSCRIPT NOREX Members discussed the platform and scope of forcing endpoint health checks; logging entries or activities to watch for to detect someone roaming the network; whether an EDR tool in use has an MDR component; types of endpoint security tools in place; moving from Cisco AMP Endpoint to Microsoft Defender Endpoint; considering Palo Alto, Microsoft, Red Canary, and other tools; CrowdStrike vs SentinelOne; SentinelOne's Rollback feature; using an USB device to block or allow policy; privacy / policy challenges with XDR (Extended Detection Response); EDR on devices traveling to China; locking down devices of terminated or remote workers; and handling unapproved software detection and removal. 27 Pages (NV2431)

IT ASSET MANGEMENT TRANSCRIPT NOREX Members discussed core investments for IT assets in 2023; successes in building an asset management program; resource levels dedicated to ITAM practices; key measures to tracking assets; foundational pieces needed before IT asset management is useful; successful ITAM tools; tracking software assets vs hardware assets; lessons learned implementing a software asset management solution; factors considered for on-prem vs Cloud-based software asset management solutions; experience with doing a formal software asset management process maturity assessment; managing endpoints for a 100% remote workforce; managing assets that do not have an agent installed; and pros / cons to a Managed Security Service. 24 Pages (NV2430)

SERVICENOW TRANSCRIPT NOREX Members discussed the reasons to select ServiceNow and moving from other toolsets; pros / cons with implementing ServiceNow; utilizing customizations within ServiceNow and experiences with customizations during system upgrades; time to implement ServiceNow; staffing model for management; end user experience via mobile usage; Configuration Management Database; Teams integration and deploying the catalog / portal to the Teams client; Employee Center; integrating ServiceNow with work-tracking systems like Azure DevOps; Software Asset Management module; ServiceNow Discovery tools; metrics to measure customer experience; and Project Management module. 28 Pages (NV2429)

EDUCATION IT ISSUES TRANSCRIPT NOREX Members discussed lessons learned while managing a school population that suddenly went remote; remote management tools used to patch and support checked- out equipment; changes in IT staffing needs when changing from on-prem to remote; downsizing Zoom licensing with the move back to mostly in-person classes; implementing Class for Zoom; applications used to manage phones and tablets coming onto campus; applications used to manage and push data to students' tablets;

helpful and / or required security certificates; Moodle LMS and other vendors such as Canvas and D2L; airSlate / signNow over DocuSign and PandaDoc; and partnering with Coursera. 12 Pages (NV2426)

VDI / DESKTOP AS A SERVICE (DaaS) TRANSCRIPT NOREX Members discussed differences between Virtual Desktop Infrastructure (VDI) and Desktop as a Service (DaaS); which is better for virtualization needs; justifying the investment in DaaS because of its agility; best use cases for DaaS; moving from Windows 10 desktops to remote work and VDI; successful deployment of Azure Virtual Desktop (AVD); utilization of VMware Horizon platform on-prem and in Azure as a hybrid configuration; utilizing Workspot DaaS; and cost analysis of DaaS vs traditional, user-device replacement schedules. 19 Pages (NV2424)

SQL SERVER TRANSCRIPT NOREX Members discussed current version of SQL Server in use; percentage of SQL workload in the public Cloud; drivers to move SQL workload to the Cloud; advantages / disadvantages of going fully virtual with SQL Server, one instance with many different databases and applications vs one virtual machine with different instances for each application; migrating from an iSeries to SQL Server; changing the default SQL port and / or encrypting all traffic; protecting SQL injections through websites; best practices around MS licensing compliance; and solutions for long-term, database growth reporting / trending. 16 Pages (NV2423)

RISK & VULNERABILITY MANAGEMENT TRANSCRIPT NOREX Members discussed conducting a formal vulnerability assessment; prioritizing which aspects of Risk / Vulnerability Management to be managed internally vs contracted out to a MSS vendor; mitigating human resources risk; reporting to executives / application owners; communicating risk to decision makers; policy to patch zero-day, critical, high, medium, or low vulnerabilities; dynamic Asset Management tools; processes used to discover and track vulnerabilities in IT systems; and measuring progress on remediating vulnerabilities. 21 Pages (NV2422)

MANUFACTURING INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed the top three business-facing projects initiated this year, metrics used to measure the performance of IT, improving IT vs the manufacturing lifecycle, the work environment for IT workers, Microsoft Compliance Manager for O365, introducing user profiles, dealing with passwords, determining support group when issues could be IT or OT, segmenting BT / IT and OT Networks, barcode scanners in a HighJump environment, solutions to track employees and visitors in facilities for emergencies, and CMMS / EAM solutions. 21 Pages (NV2421)

DISASTER RECOVERY / BUSINESS CONTINUITY TRANSCRIPT NOREX Members discussed organizational roles, responsibilities, and accountability for DR / BC; defined standards; having DR and BC sites on-prem, Cloud, or colocation; DRaaS vendors; backup solutions such as VEEAM, Acronis, and MS Azure; strategies for having both a DR and a BC site; replication software; Oracle; established reusable patterns; incorporating DR / BC plans in architecture reviews; app tiers / categories corresponding to implementation; meeting business requirements for resiliency and performance; and testing disaster recovery plans. 24 Pages (NV2418)

ENERGY / UTILITY INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed IT budget trends, applications used to track compliance requirements, tools to analyze historical meter and weather data to determine the performance of behind-the-meter load control programs, leveraging collaboration tools (MS Teams / Slack) to work with 3rd parties, vendor partners, or stakeholders, use of MS Sentinel as both a SIEM and a SOAR, network tap monitoring tools like CyberX and Darktrace, Identity and Access Management initiatives, maintaining utility-owned communications equipment, partnering with outside Incident Response Services, and capabilities in the area of RPA / Automation. 22 Pages (NV2412)

TALENT RECRUITMENT / MANAGEMENT / RETENTION TRANSCRIPT NOREX Members discussed top-shelf benefits today's IT candidates expect, strategies implemented to retain current talent, challenges with pushing IT employees to return to the office, available hybrid / work-from-home / in-office options, creating bonus programs, targeting and hiring talent that is a cultural fit and has the required skill set, measuring technical knowledge vs what is listed on a resume, questions candidates ask about the hiring organization, promoting employee engagement, and creating a team atmosphere when many employees continue to work remotely. 18 Pages (NV2411)

RUSSIA-UKRAINE IMPACT ON CYBERSECURITY TRANSCRIPT NOREX Members discussed trusting the resiliency of government and infrastructure security, increase in security metrics due to the war, measuring the risk impact of this event, determining dependencies and risks with overseas vendors, important steps of system hardening, email security vendors, utilizing threat intelligence effectively, preparing executives for worst-case scenarios, Honeypot as a security measure, supply chain attacks, securing Operational Technology environments, and the evaluation and address of risks from ransomware. 22 Pages (NV2410)

CONSTRUCTION INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed PMO for IT, challenges with finding and retaining IT talent, internal vs outsourced onsite technical support, 5G connectivity, equipment used besides individual phones / tablets, WebDAV, WordPress for intranet, utilizing interactive, large-format displays such as the Dell 55" on jobsites, and security cameras used onsite. 21 Pages (NV2408)

HELP DESK / SERVICE DESK TRANSCRIPT NOREX Members discussed outsourcing vs insourcing the Service Desk function, IT Service Providers, tracking and reporting key metrics / KPIs, response and resolution targets for Incident Ticket severity levels, the role of the individual answering incoming calls to the Help Desk, the structure of the Help Desk team, best practices for SLAs on Level 2 & Level 3 service requests, dealing with inappropriate escalations, Tier 1 staff engagement, training and professional development, VDI, and Self-Service. 32 Pages (NV2407)

NETWORK MANAGEMENT / MONITORING / REFRESHES TRANSCRIPT NOREX Members discussed network management trends for 2022, the frequency to push out configuration changes, improvements to network monitoring to increase cybersecurity, partnering to monitor and manage infrastructure monitoring, network performance and diagnostic products in use, toolsets used to assess and monitor network capacity, network monitoring solutions for remote access, open source network management solutions, KRI / KPI metrics, and migrating business applications and data to a hybrid Cloud environment. 21 Pages (NV2404)

IAM: MANAGING INDENTITIES & PROVISIONING TRANSCRIPT NOREX Members discussed lessons learned from implementing an IAM solution, the source of truth for employee information and identity, tools used on MFA privileged accounts, tools for account provisioning for Active Directory / Hybrid 365, IAM tools in use to manage user accounts, staff resources devoted to IAM, and Access Reviews / Certifications. 16 Pages (NV2405)

TRANSPORTATION INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed the shortage of drivers, issues with finding and retaining IT workers, addressing cybersecurity risk, types of digital investments being made, managing the 3G February / March sunset dates and asset tracking, implementing Snowflake for a data warehouse solution using Azure Data Factory for ELT / ETL, solutions for source control, data dictionary, glossary of terms while following DevOps best practices, and increased infrastructure and maintenance costs. 16 Pages (NV2403)

SECURITY INITIATIVES FOR 2022 TRANSCRIPT NOREX Members discussed the percentage of the IT budget directed to InfoSec, cyber insurance, top 3 security initiatives, implementing a governance framework for accepting risk, GRC tools, best practices to apply security patches on Windows OS, automating / outsourcing cybersecurity processes, MDR services and pen testing, successful tools to protect from malicious web links and sites, VPN requirements, EDR / AI scanners, security strategies, and providing security dashboards to company officers. 28 Pages (NV2401)

HOSTED ERP SOLUTIONS TRANSCRIPT NOREX Members discussed whether shifting to the Cloud is the right move when an organization is primarily on-prem, integrating Cloud applications with an ERP, utilizing Boomi as an integration Platform as a Service (iPaaS), value-add with an external PM to help push ERP implementation, security concerns with sensitive data on someone else’s Cloud, using Microsoft Dynamics Business Central, Oracle R12.2.5 on-prem and moving to Oracle Cloud, and utilizing a Cloud-based ERP for operations in China / South Korea. 17 Pages (NV2398)

MULTI-FACTOR AUTHENTICATION / SINGLE SIGN-ON TRANSCRIPT NOREX Members discussed struggles setting up users with MFA, conditional access policies, minimizing the impact to registration of the users before enabling 2FA / MFA, experiences implementing Duo 2FA, passwordless MFA configured through Microsoft Azure, integrating with Remote Desktop Connection to servers and / or Terminal Server, MFA products for remote access to network (VPN / RDP) and local login, adopting Single Sign-On for 3rd-party accounts, and pain points with implementing OKTA for MFA and SSO. 19 Pages (NV2396)

PATCH MANAGEMENT TRANSCRIPT NOREX Members discussed efficient patching and vulnerability scan frequency, maintenance window downtime, patch management for servers needed for production environments that have zero downtime, patch management on company desktops / laptops for remote users, time to delay patching before forcing the user, Linux patch automation, software tools to manage patching process, open source patch management for Windows, logging changes for monthly workstation patching, and processes used to evaluate patches from vendors. 27 Pages (NV2394)

CYBERSECURITY TRANSCRIPT NOREX Members discussed how best to prepare for a ransomware attack, steps to take when hit, security teams reporting risk, incident response plans, managing vulnerabilities, best ways to combat phishing and malware attacks, KnowBe4 for cybersecurity and phishing awareness platform, training, Cybersecurity Awareness Month to raise awareness, Microsoft Defender vs Symantec / Norton, endpoint protection, evolution of threats in work-from-home models, and security threats in the Cloud. 31 Pages (NV2392)

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 Scrum Masters, 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: WFH 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 session. 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 session. 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 session. 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 session. 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, & 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 session. 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 session. 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 session. 19 Pages (NV2337)

CYBERSECURITY TRANSCRIPT NOREX Members share cybersecurity best practices and tool recommendations during this July 2020 session. 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 session. 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 session. 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 session. 20 Pages (NV2323)

MICROSOFT TEAMS GOVERNANCE TRANSCRIPT NOREX Members and guests share their experience, questions, and ideas on Microsoft Teams. This session 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 session, 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 session. 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 session. 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 session. 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 session. 15 Pages (NV2298)

HELP DESK / SERVICE DESK TRANSCRIPT NOREX Members discuss Help Desk / Service Desk procedures and recommended tracking tools during this November 2019 session. 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 session. 10 Pages (NV2289)

VULNERABILITY MANAGEMENT TRANSCRIPT NOREX members share recommendations on processes and tools to manage IT vulnerabilities and risks during this September 2019 session. 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 session. 22 Pages (NV2287)

DOCUMENT MANAGEMENT TRANSCRIPT NOREX members share experiences selecting, implementing and managing Document Management systems during this September 2019 session. 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 session. 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 session. 25 Pages (NV2283)

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

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

WEB CONTENT MANAGEMENT TRANSCRIPT NOREX members had good discussion during this May 2019 session. 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 session. 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: SERVICENOW TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed module usage; managing and communicating features and releases; staffing requirements; customization impact; requests requiring multiple organizational pillars; APM considerations; CMDB and CSDM interaction; usage of Automated Test Framework; Release Management Module; use of the employee portal; integration with Microsoft Teams; data extraction tips; usage of archive function; incident response functionality; backup options; ServiceNow Impact Squad; and citizen development implementation. 19 Pages (NS253)

SELECT: RISK & VULNERABILITY MANAGEMENT NOREX Select Members from Fortune / Forbes 1000 organizations discussed including SLAs in a strategic approach; prioritizing vulnerabilities; tracking tools; identifying shadow IT; measuring program effectiveness; internal communication; emerging threats; and communicating risk to senior management. 12 Pages (NS250)

SELECT: MANAGING TECHNICAL DEBT TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed the definition, management, and communication of technical debt; how to identify, surface, and prioritize TD; risk as an assessment; using employee retention as leverage; management in the Cloud vs on-prem; IT in the enterprise hierarchy; and balancing TD and product development. 15 Pages (NS247)

SELECT: MANAGING SHADOW IT TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed root causes for shadow IT; the balance between “lock down” and “user friendly”; having policies and programs overruled; incorporating shadow IT into enterprise IT management; tools for detection and visibility; moving from monitoring to enforcement; and WhatsApp. 13 Pages (NS236)

SELECT: SECURITY INCIDENT RESPONSE TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed developing an incident response plan; incident communication tips; tabletop exercise recommendations; usage of an incident response service provider; business continuity tool recommendations; post-breach activity; third-party security monitoring; and incident response playbooks. 13 Pages (NS243)

SELECT: APPLICATION MANAGEMENT TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed developing a business application catalog: the use of ServiceNow; application tracking and data synchronization; automating processes; user education on the latest apps, tools, and features available for use; identifying a source of truth; asset management; and outsourcing asset management. 11 Pages (NS242)

SELECT: BUSINESS RESILIENCY TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed business continuity vs business resiliency; business resiliency framework; escalating incident response to crisis management; value of business continuity to organization in post-COVID world; guiding principles regarding manufacturing autonomy and resiliency; hybrid / remote work affecting alternate site strategy; and storing DR documented processes / runbooks so they are easily accessed during an event. 15 Pages (NS240)

SELECT: IT GOVERNANCE TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed initiating a governance process; the scope of IT Governance; defining IT Governance; decision makers and how decisions are made; establishing governance standards; IT Governance tools; Change

Management considerations; maintaining process; and dealing with a less-rigid planning cycle. 13 Pages (NS238)

SELECT: SERVICENOW CMDB TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed CMDB licenses and application recognition; how detailed a CMDB can get; challenges navigated on CMDB practices and implemented capabilities that rely on CMDB data cleanliness; tips to set up Multisource CMDB; experiences with interfacing / integrating external CMDBs or external discovery tools; automatic import capabilities from other sources like Microsoft Active Directory or Microsoft System Center Configuration Manager; successfully implementing a true CMDB with relationships between CIs; master data strategy for end-to-end integration across CMDB, Incident Response Management, EA tools, and PMO tools; assigning capabilities to applications or services; and how deep in the CSDM model you define information. 18 Pages (NS235)

SELECT: MICROSOFT 365 / TEAMS TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed Unified Communication strategy; operationalizing the rapid changes in M365; use cases for a Team vs a Channel; the Wiki app to provide a knowledge base of articles; integrating Records Retention Schedule (RRS) into MS Teams / SharePoint / OneDrive; workarounds used if MS Teams / SharePoint / OneDrive is unavailable; integrating Azure / Azure AD with M365; processes used to manage business requests to add Teams apps; managing access in the SharePoint site that comes automatically with a Team; and internal support structure implemented to support Teams / M365 within IT and / or the business. 13 Pages (NS234)

SELECT: VENDOR RISK MANAGEMENT TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed driving security improvements and measuring results among vendors and suppliers; how Vendor Risk Assessment activities are performed and what results from that activity; what portions of the vendor survey add the most value; what departments in an organization should be included to assess the Vendor Risk Assessment; the process for creating on-site or remote assessment in addition to vendor assessment; proper responses to poor performance, vendor-caused incidents, business disruptions, and negative financial impact; third-party training before onboarding; fourth-party compliance; process for vendor to submit notification of system maintenance or changes; and management of lifecycle from initiation to off-boarding vendors. 19 Pages (NS232)

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)

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)

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

IT TRENDS 2023 Q4 IT Trends is a collection of the NOREX Member input captured in the fourth quarter of 2023 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 25 Pages (DT2023-4)

IT TRENDS 2023 Q3 IT Trends is a collection of the NOREX Member input captured in the third quarter of 2023 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 22 Pages (DT2023-3)

IT TRENDS 2023 Q2 IT Trends is a collection of the NOREX Member input captured in the second quarter of 2023 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 36 Pages (DT2023-2)

IT TRENDS 2023 Q1 IT Trends is a collection of the NOREX Member input captured in the first quarter of 2023 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 45 Pages (DT2023-1)

IT TRENDS 2022 Q4 IT Trends is a collection of the NOREX Member input captured in the fourth quarter of 2022 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 37 Pages (DT2022-4)

IT TRENDS 2022 Q3 IT Trends is a collection of the NOREX Member input captured in the third quarter of 2022 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 44 Pages (DT2022-3)

IT TRENDS 2022 Q2 IT Trends is a collection of the NOREX Member input captured in the second quarter of 2022 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 43 Pages (DT2022-2)

IT TRENDS: 2022 Q1 IT Trends is a collection of the NOREX Member input captured in the first quarter of 2022 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 57 Pages (DT2022-1)

IT TRENDS: 2021 Q4 IT Trends is a collection of the NOREX Member input captured in the fourth quarter of 2021 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 44 Pages (DT2021-4)

IT TRENDS: 2021 Q3 IT Trends is a collection of the NOREX Member input captured in the third quarter of 2021 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 59 Pages (DT2021-3)

IT TRENDS: 2021 Q2 IT Trends is a collection of the NOREX Member input captured in the second quarter of 2021 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 56 Pages (DT2021-2)

IT TRENDS: 2021 Q1 IT Trends is a collection of the NOREX Member input captured in the first quarter of 2021 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 57 Pages (DT2021-1)

IT TRENDS: 2020 Q3 & Q4 IT Trends is a collection of the NOREX Member input captured in the third and fourth quarters of 2020 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 74 Pages (DT2020-2)

IT TRENDS: 2020 Q1 & Q2 IT Trends is a collection of the NOREX Member input captured in the first and second quarters of 2020 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 62 Pages (DT2020-1)

CIO: ALIGNING BUSINESS & TECHNOLOGY PLANNING TRANSCRIPT NOREX Members discussed stakeholder involvement in planning; usage of a steering committee; technology roadmap tools; capability mapping; consultant involvement; organizational considerations; business-led ERP implementation; steps to achieve IT objectives; digital transformation and ChatGPT usage; cyber training for leadership; retaining staff; and transferring IT leadership. 17 Pages (CV083)

CIO: IT DEPARTMENT KPIs TRANSCRIPT NOREX Members discussed metrics shared with Executive Leadership to show IT department’s value, common KPIs tracked, performance-level KPIs tracked other than

MTTA and MTTR, creating a balanced scorecard for infrastructure, help desk and application development, total tickets vs open tickets, measuring customer satisfaction rates, KPIs and data interpretations of security- related issues, key performance indicators to monitor with Managed Security Service Providers, monitoring the effectiveness of patching program, IT ROI, IT expenses, and identifying your cost breakdown. 26 Pages (CV080)

CIO: IT BUDGETING & PLANNING FOR 2022 TRANSCRIPT NOREX Members discussed projecting vendor price increases, cybersecurity goals aligning with legal and cyber insurance needs, percentage of IT budget to overall budget, success stories to acquire more funding and staff, the cost to move to the Cloud, software, infrastructure, and platforms when moving to the Cloud, leveraging ARPA funding in 2022, mid-year reviews to analyze spending, determining the optimal size for an IT organization, critical-success criteria, and measuring productivity of software developers in an Agile Scrum environment. 24 Pages (CV078)

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 session. 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)