Toolkit

The Vendor-Free IT Community.

MOBILE DEVICE MANAGEMENT

These NOREX Member-contributed documents include policies, evaluations, agreements, Member polls and peer discussions, and document on stipends, allowances, BYOD, and security. | TK007

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

BYOD

BYOD & MOBILE POLICY. The policy defines eligibility and regulates the reimbursement to employees requiring a mobile device for company business. 8 Pages (20-781)

BYOD POLICY. Procedures on eligibility, security, connectivity support, privacy, authorized use, and company stipends are covered in this policy. 4 Pages (20-719)

BYOD POLICY. Policy mandates that only eligible employees with particular job requirements be granted the privilege of purchasing / using their own smart phones and tablets for business. 2 Pages (20-576)

BYOD ACKNOWLEDGEMENT. This agreement should be signed when an employee elects to use his / her personally-owned mobile device, laptop, or tablet for business purposes. 1 Page (20-570)

BYOD USER AGREEMENT. The following agreement applies to mobile devices used for business purposes. 2 Pages (20-324)

Discussions

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

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

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

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

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

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

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

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

GLOBAL IT ISSUES TRANSCRIPT. NOREX Members discussed the biggest issues they and their organizations are facing with a global footprint in today's business climate. The expectations with employees able to return to the office, IT talent recruiting and hiring internationally, standardization of processes, cybersecurity, procuring equipment globally, keyboard sourcing, and in-country IT support were challenges shared by all Member participants. 17 Pages (NV2371)

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

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

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)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

HELP DESK / SERVICE DESK TRANSCRIPT. Recent moves of entire workforces home has put a great deal of pressure on the Help Desks/Service Desks within companies. During this WebForum, NOREX members discuss the challenges and successes of those moves and the move back, metrics and how they are evolving and tools and training that members are using to service their organizations. This transcript includes a large discussion around tools, help desk to employee ratios and a robust chat log conversation. 33 Pages (NV2318)

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

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

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

PREPARATION FOR A REMOTE WORKFORCE TRANSCRIPT. With the onset of COVID-19 and the need for distancing, aggressive remote workforce processes are in place for most NOREX Member organizations.

NOREX hosted this discussion on March 17, 2020 with over 200 participants. This transcript includes a very active chat log conversation, results from polls taken, and the takeaways we received from those who completed an evaluation. 48 Pages (NV2313)

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

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

MICROSOFT TEAMS AND ALTERNATIVE SOLUTIONS TRANSCRIPT. Microsoft Teams and alternative solutions is a strong, growing area of interest for many NOREX Members. This discussion covers adoption and implementation, benefits and shortfalls, use of chat and collaboration, developing MS Teams governance, and more. Polls, links and an in-depth chat section is included in this February 2020 transcript. 32 Pages (NV2308)

PANDEMIC CRISIS PREPAREDNESS TRANSCRIPT. NOREX members discuss business continuity, disaster recovery and updated policies to prepare for the possibility of a pandemic. 12 Pages (NV2307)

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

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

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

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

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

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

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

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

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

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

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

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

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

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)

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: NAVIGATING INTERNATIONAL / GLOBAL IT ISSUES DURING A PANDEMIC TRANSCRIPT. During this CIO call, NOREX Members and guests shared experience and ideas on global office management, particularly in Asia. They discussed differences in products, regulations, firewalls, long distance connectivity, and collaboration tools. 21 Pages (CV074)

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

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

Laptops / Tablets

QUARTERLY LAPTOP / TABLET CHECKUP FORM. This form ensures laptops and tablets used by employees for extended periods of time are kept in good physical condition and that updates and patches have been applied on a regular basis. 1 Page (20-572)

LAPTOP CHECK-IN CHECK-OUT FORM. This template records both check-in and check-out of company owned devices for temporary use. 1 Page (20-568)

LAPTOP / TABLET USE JUSTIFICATION. Requests for employee use of laptops and / or tablets can be logged according to justification level using this form. 1 Page (20-567)

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)

Mobile Access & Connectivity

ROLE-BASED MOBILE POLICY. This document lays out the options, eligibility, and assignment process for employee mobile devices. 2 Pages (20-1023)

MOBILE DEVICE STANDARD. This standard defines the appropriate use and security configuration of mobile devices. 2 Pages (20-1022)

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)

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

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)

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)

REMOTE WORK POLICY. This policy provides employees with the standards and procedures related to a remote work arrangement. 5 Pages (20-756)

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)

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

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)

REMOTE ACCESS POLICY. Defined here is the procedure to remotely access the company network from an external network not under the control of the company. 5 Pages (20-556)

Policies

MOBILE PROVISIONING GUIDELINES. Provisioning, budgeting, oversight, and user responsibility are outlined in this cell phone policy. 2 Pages (20-1020)

PERSONAL MOBILE DEVICE POLICY. This policy provides guidelines for users accessing company systems or information using a personal mobile device. 3 Pages (20-1019)

MOBILE PHONE AND DEVICE POLICY. This policy describes the proper, appropriate, and safe use of cell phones and mobile devices. 2 Pages (20-1018)

MOBILE DEVICE USAGE. This policy governs the use of all portable electronic devices, tablets, cell phones, and laptops, regardless of ownership. 8 Pages (20-994)

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

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

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

WIRELESS DEVICE & SERVICE POLICY. This policy establishes guidelines for acquisition, possession, monitoring, and appropriate use of wireless devices and services. 4 Pages (20-770)

MOBILE DEVICE POLICY. Provided here is guidance for full-time employees connecting personal mobile devices to the wireless network. 3 Pages (20-750)

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)

TEXTING POLICY. The following is a secure texting standard for communicating protected or other restricted information. 3 Pages (20-665)

SECURE TEXTING USING THE SPOK APP. A hospital environment describes using the Spok mobile app for secure texting and activating STEMI alerts in their facilities. 2 Pages (20-664)

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

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

MOBILE DEVICE USER POLICY. This agreement is necessary to help ensure proper protection of company confidential information accessed through mobile devices. 2 Pages (20-575)

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)

CORPORATE MOBILE POLICY. This policy governs the use of mobile devices whether company-owned or approved corporate data access from a personally owned mobile device. 8 Pages (20-483)

ELECTRONIC COMMUNICATION POLICY. This document outlines the policies and procedures that govern all company electronic communication systems. 5 Pages (20-481)

MOBILE DEVICE USE POLICY. This policy provides guidelines for users accessing company systems or information utilizing a mobile device. 3 Pages (20-480)

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)

INTUNE POLICY. The following template informs employees about company policy on the use of Microsoft Intune for centralized management of mobile devices. 2 Pages (20-457)

CORPORATE MOBILITY POLICY. This policy is designed to enable eligible employees to manage business mobile connectivity costs and govern the use of mobile devices. It supports BYOD and corporate sponsored plans and covers data privacy requirements such as GDPR. 15 Pages (20-449)

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

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

MOBILE DEVICE USAGE. This publication covers responsibility & authority, procedures, and expectations pertaining to all mobile devices and their use. 8 Pages (20-370)

MOBILE DEVICE POLICY. This policy ensures Information Systems department standards & practices are maintained with regard to the usage of mobile devices connecting to company networks and systems. 3 Pages (20-369)

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

SAFE TECH MOBILE DEVICE GUIDELINES. This document is intended to provide safe technical mobile device guidelines and to provide background on handling technical mobile device situations. 6 Pages (20-351)

RETAIL MOBILE DEVICE SURVEY. The following are from a survey completed by retail organizations, with results in BYOD, device policies, MDM applications, and stipends. 8 Pages (20-348)

MDM POLICY. Mobile Device Management (MDM) is a software application that secures, monitors, manages, and supports mobile devices across the enterprise. 7 Pages (20-326)

MOBILE DEVICE USAGE. This policy outlines responsibilities, privacy, and procedures regarding the use of smart phones and other mobile devices. 7 Pages (20-325)

MOBILE DEVICE POLICY. This policy governs the use of mobile devices for business purposes and defines the appropriate use and security configuration of personal devices which are granted access to the company network and computer systems. 7 Pages (20-292)

WIRELESS ACCESS POLICY. Internal, Guest, and BYOD access networks each have different but similar connectivity regulations, as explained in this policy. 1 Page (20-291)

TELENETWORKING/MOBILE POLICY. This policy defines control requirements for access to information resources and applies to employees and non-employees who access information resources remotely. 3 Pages (20-290)

MOBILE DEVICE POLICY. Covering OYOD (Own-Your-Own-Device) or company-owned devices, this policy can be tailored to fit your own needs. 4 Pages (20-038)

RESPONSIBLE IT RESOURCE USE. Valuable Information Technology resources are monitored and controlled though the policies contained in this document. 10 Pages (20-037)

CELLULAR DEVICE POLICY. This policy establishes guidelines for the issuance and usage of company-owned cellular devices as well as the administrative issues relating to device acquisition and reimbursement.
5 Pages (50-254)

Polls

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

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

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

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

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

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

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

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

Requests & Agreements

MOBILE DEVICE PURCHASE REQUEST. This template is for employees who wish to request a company subsidized purchase of a smartphone, tablet, or other mobile device. 2 Pages (20-928)

WIRELESS DEVICE USE AGREEMENT. Terms and conditions for employee owned and company owned wireless devices are explained and agreed to using this form. 3 Pages (20-718)

QUARTERLY LAPTOP / TABLET CHECKUP FORM. This form ensures laptops and tablets used by employees for extended periods of time are kept in good physical condition and that updates and patches have been applied on a regular basis. 1 Page (20-572)

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

MOBILE DEVICE AGREEMENT. Terms and conditions for the use of company or personally-owned mobile devices are outlined in this agreement. 4 Pages (20-569)

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)

RFP: MOBILE WIRELESS SERVICES. To meet current and future communication needs, the company is requesting proposals from qualified mobile communications firms to provide nationwide mobile voice & data services and equipment for a period of two years with two additional one-year options. 8 Pages (20-258)

Security

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

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

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

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

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

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

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

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

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

CYBERSECURITY FRAMEWORK. This section addresses the overall Strategic Plan associated with cyber related controls, plus the general steps to be followed in the event of a cyber security attack against data or systems. 7 Pages (20-358)

SAFE TECH MOBILE DEVICE GUIDELINES. This document is intended to provide safe technical mobile device guidelines and to provide background on handling technical mobile device situations. 6 Pages (20-351)

iPHONE MDM. Explored here are solution options for the return and/or unlocking of an employee iPhone, BlackBerry, or other mobile device specifically with use of the "find my phone" function. 3 Pages (20-167)

iPHONE RESTRICTION TEMPLATE. This is a list of common iPhone (and other mobile device) features and applications that potentially need permissions or restrictions in the business setting. 1 Page (20-161)

Stipends / Allowances

MOBILE DEVICE STIPEND MODELS. This document describes three models used for mobile device stipends. 1 Page (20-931)

CELL PHONE REIMBURSEMENT. This policy outlines the rules for cell phone expense reimbursement when there is a defined a business requirement for use of a device. 2 Pages (20-915)

PHONE REIMBURSEMENT POLICY. This policy explains eligibility requirements and the procedure for requesting reimbursement. Also included is an acknowledgement form. 2 Pages (20-509)

REMOTE OFFICE STIPEND POLICY. This policy defines the necessary criteria and process for full time work-from-home employees to receive monthly stipend payment to use their personal computer equipment for job performance. 3 Pages (20-389)

MOBILE PHONE STIPEND POLICY. This document explains the way the company will pay for or reimburse cell phones, mobile device service plans, and who qualifies to get reimbursement. 5 Pages (20-373)

CELL PHONE STIPEND AGREEMENT. A cell phone stipend will be determined based on employees' job duties and responsibilities. 1 Page (20-372)