POLICIES & PROCEDURES

These NOREX Member-contributed documents include acceptable use, Cloud computing, data management, email, equipment, HR, personnel, incident management, mobile computing, network access, password, project / change management, records management, remote access, security, social media, storage, WFH, and vendor management. | TK009

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

COPILOT TERMS OF USE Users and administrators share responsibility for the proper use of Microsoft Copilot use for protecting company data and processes. 3 Pages (20-1397)

USB DEVICE CONTROL AND USE POLICY Standards, procedures, and restrictions for employees, workers, and contractors connecting portable removable media to company resources. 2 Pages (20-1395)

ACCEPTABLE USE POLICY This policy stipulates constraints and practices that a user must agree to for access to a corporate network and other organizational assets. 3 Pages (20-1394)

AI ACCEPTABLE USE POLICY This policy defines the appropriate use of Artificial Intelligence technologies to protect the company, its employees, and its stakeholders from any harm resulting from the misuse of AI. 2 Pages (20-1381)

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)

AI ACCEPTABLE USE POLICY This policy establishes guidelines on AI tool use, to prevent leaks of confidential data and ensure the tools are used appropriately, ethically, and legally. 2 Pages (20-1284)

DATA USE AGREEMENT This template is an agreement for limited data use between two or more parties and is HIPAA compliant. 2 Pages (20-1242)

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)

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

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

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)

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)

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)

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

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

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)

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)

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

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

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)

Business Continuity / Disaster Recovery

BACKUP AND RESTORATION POLICY This policy provides a means to actively manage risks associated with data loss by defining a sound backup regime for all data services. 6 Pages (20-1283)

BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY This document defines policy directive on business continuity activities, including planning for all critical business processes and service activities. 7 Pages (20-1282)

BUSINESS CONTINUITY PLAN SIMULATION REPORT This template demonstrates the outcome of annual simulation exercises as part of ongoing maintenance of Business Continuity Plans (BCP). 10 Pages (20-1281)

BUSINESS CONTINUITY PLAN TABLETOP PREPARATION This document is a template of the procedures used during a Business Continuity Plan (BCP) tabletop exercise. 13 Pages (20-1280)

IT DATA CENTER AND COLOCATION POLICY Guidelines for proper maintenance and protection of the data center, whether hosted in-house or offsite, are provided in this policy. 3 Pages (20-1068)

BUSINESS CONTINUITY POLICY This policy includes details on data backup, retention, destruction, colocation, and disaster recovery. 4 Pages (20-1062)

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

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

DISASTER RECOVERY PROCEDURE OUTLINE The following is a basic outline of disaster recovery site procedures. 1 Page (20-678)

DISASTER RECOVERY & BUSINESS CONTINUITY POLICY TEMPLATE A disaster recovery & business continuity policy includes processes for recovering critical technology systems and data. 3 Pages (20-667)

Change Management

CHANGE MANAGEMENT PROCESS These workflows show one organization's change management process. 5 Pages (20-1375)

CHANGE MANAGEMENT POLICY This policy describes the procedures employed to track and approve modifications to enterprise IT systems, technologies, supporting infrastructure, and solutions. 3 Pages (20-1064)

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

CHANGE REQUEST PROCEDURE This process includes the information needed to classify the change type, the appropriate level of communication based on change, and how to document the change. 9 Pages (20-762)

CHANGE MANAGEMENT POLICY By having a formal change process in place, the impacts of proposed changes are better understood and the negative impacts of changes are minimized. 3 Pages (20-761)

IT CHANGE MANAGEMENT POLICY This policy provides standard procedures for managing change requests in an agile & efficient manner. 2 Pages (20-704)

CHANGE MANAGEMENT POLICY This policy is designed to provide a process for requesting and managing changes to business applications and other business critical systems created or maintained by the IT department. 3 Pages (20-578)

CHANGE MANAGEMENT POLICY This Change Management process will assess the impact and risks of change, and document, identify, define, and formalize processes involved. 11 Pages (20-346)

IT CHANGE MANAGEMENT POLICY This policy shall cover all changes which have an impact to a business unit, business function, or IT service. 2 Pages (20-156)

CHANGE MANAGEMENT GUIDE A four-phased approach to Change Management is described in this manual of tips, resources, and samples. 27 Pages (20-331)

PROJECT CHANGE FORM This form is used to describe changes and their impact to the project, as well as acceptance criteria. 2 Pages (50-440)

IT CHANGE MANAGEMENT PROCESS The change management process helps control the life cycle of strategic, tactical, and operational changes to IT services through standardized procedures. 12 Pages (50-427)

TECHNOLOGY CHANGE ADVISORY BOARD CHARTER This charter describes the role of the technical management committee responsible for reviewing and approving changes to the technology environment. 2 Pages (50-419)

GLOBAL IT CHANGE MANAGEMENT PROCESS This document describes a globally consistent IT change management process based on ITIL best practices. 18 Pages (50-407)

IT CHANGE MANAGEMENT STANDARD This document presents Change Management practices, under the umbrella of IT Service Management, to be adopted and practiced by IT employees and those employees whose changes fall under the oversight of IT Change Management. 14 Pages (50-247)

Cloud Computing

CLOUD COMPUTING POLICY This policy establishes the minimum requirements for securing company information that is processed, stored, or accessed through outsourced via the Internet. 3 Pages (20-484)

ONEDRIVE CLOUD STORAGE POLICY This policy establishes guidelines regarding support and usage of the authorized OneDrive Cloud Storage. 8 Pages (20-230)

CLOUD COMPUTING POLICY This policy outlines the Cloud computing requirements and how they apply to the company and its subsidiaries. 4 Pages (20-049)

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

Data Management

VENDOR PRIVACY ASSESSMENT TEMPLATE This assessment provides a robust guide to assess the nature of the vendor's technology and its use of personal information. 4 Pages (20-1372)

VENDOR PRIVACY ASSESSMENT PROCEDURE This procedure is used as a guide when evaluating vendors for data-driven programs, initiatives, or projects as a part of your privacy management program. 13 Pages (20-1371)

PRIVACY IMPACT ASSESSMENT TEMPLATE Use and disbursement of private information is assessed with this Privacy Impact Assessment (PIA) for each initiative, program, application, or system. 8 Pages (20-1370)

PRIVACY IMPACT ASSESSMENT PROCEDURE This procedure assists staff in developing, monitoring, and reviewing Privacy Impact Assessments. 5 Pages (20-1369)

PRIVACY BREACH RESPONSE PROCEDURE This is a process for responding to a privacy incident or breach, from initial investigation to debriefing if a breach has occurred. It includes details about essential team members and external experts who may respond to a privacy breach. 14 Pages (20-1368)

PRIVACY BREACH RESPONSE POLICY Described here are the various roles that have a responsibility in breach readiness and response. 7 Pages (20-1367)

PRIVACY DATA MANAGEMENT POLICY These are steps taken by the Privacy Office responding to requests for access to, correction of, or deletion of personal information, as well as complaints about privacy practices. 8 Pages (20-1366)

ORG PRIVACY POLICY This privacy policy governs collection, use, and disclosure of personal and personal health information. This includes profile, contact details, professional, technical, financial, survey, and communication data. 9 Pages (20-1365)

PRIVACY GOVERNANCE FRAMEWORK This framework sets out guiding privacy and responsible innovation principles as well as the enabling infrastructure. It explains the core mandate and function of the privacy program. 6 Pages (20-1364)

EMPLOYEE PRIVACY POLICY Collection, storage, and sharing of personal employee information are outlined in this policy. 9 Pages (20-1363)

ANALYTICS STRATEGY RECOMMENDATION This document explores establishment of a data strategy, timeline, staffing models, and roles for data governance. 18 Pages (20-1319)

DATA ARCHITECTURE PLAN PRESENTATION This presentation demonstrates the necessity of DAP preferred management practices, information lifecycle, and expected benefits. 12 Pages (20-1288)

DATA ARCHITECTURE PLAN This plan is a set of rules, policies, and standards that govern and define the type of data collected and how it is used, stored, managed, and integrated. 20 Pages (20-1287)

DATA STEWARDSHIP RACI MATRIX This matrix provides a layout for the Responsible, Accountable, Consulted, Informed method of outlining components of data stewardship duties. 1 Page (20-1265)

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)

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

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

DATA SHARING STANDARD This policy is aimed at creating a cooperative culture that will encourage responsible sharing of data and the removal of barriers to sharing data whenever possible. 3 Pages (20-174)

DATA SHARING GUIDELINES This guideline provides minimum requirements for an agency to use the Enterprise Service Bus (ESB) and outlines the criteria to establish an electronic interface. 12 Pages (20-175)

DATA CENTER ACADEMY COURSES This is an example of a data literacy program, listing appropriate courses and timeline. 69 Pages (50-405)

DATA LITERACY PROGRAM This presentation outlines the data literacy program, the team members involved, their roles, and education tracks. 5 Pages (50-404)

Electronic Communication

ELECTRONIC COMMUNICATIONS POLICY This policy applies to all company-provided media and services, including computers, email, and internet. 4 Pages (20-1392) (TK2 POLICY, TK5 POLICY, TK9 ELEC.)

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

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)

SHAREPOINT GOVERNANCE POLICY This policy defines requirements, processes, roles, and responsibilities for SharePoint environment development and administration. 5 Pages (20-1203)

MS TEAMS GOVERNANCE AND POLICY Microsoft Teams naming, organization, features, compliance, and security are presented in this policy. 10 Pages (20-1037)

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)

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

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)

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)

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)

PHISHING EMAIL POLICY Forged or faked electronic documents and email, 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)

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

FAXING POLICY & PROCEDURE The transmission of Protected Health Information (PHI) by fax or e-Fax. 4 Pages (20-405)

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

EMAIL & DATA RETENTION The following is an email retention policy and a general data retention policy overview. 3 Pages (20-355)

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

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

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

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

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)

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

Equipment / Asset Management

HARDWARE REQUEST FORM These screen shots show a process for submitting a hardware service request. 2 Pages (20-1336)

MEDIA DESTRUCTION The following are practices for digital and paper media destruction. 2 Pages (20-1317)

COMPANY EQUIPMENT AGREEMENT The following is an agreement for the care and return of company- owned equipment such as iPads or laptops. 1 Page (20-1240)

EQUIPMENT RETURN AGREEMENT This agreement covers the return of company-owned equipment in the event of employee resignation or termination. 1 Page (20-1239)

DEVICE AND MEDIA REUSE AND DISPOSAL This outlines the reuse or disposal of encrypted hard drives on work devices. 1 Page (20-1237)

DISK WIPING Effective methods for clearing and purging desktops and server drives are listed here. 2 Pages (20-1084)

DATA DESTRUCTION POLICY This document describes data destruction procedures as specified by NIST's three categories of data sanitization. 1 Page (20-1083)

MOVING YOUR DESKTOP COMPUTER This document describes disconnection and reconnection of desktop computers, monitors, and their accessories. 8 Pages (20-1069)

ASSET MANAGEMENT POLICY This policy describes management of the acquisition, use, assignment, release, and disposal of IT assets. 3 Pages (20-1065)

INFORMATION MANAGEMENT SOP This document states company policy on how computer systems within an FDA regulated company are to be brought into service, changed, maintained, and retired. 10 Pages (20-868)

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

ASSET NAMING STANDARDS A method for PC, network, & server naming standards is given below. 2 Pages (20-699)

ELECTRONIC EQUIPMENT DISPOSAL POLICY This policy stipulates procedural practices for electronic equipment and software disposal. 3 Pages (20-532)

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

LIFECYCLE MANAGEMENT PROCESS This document includes the lifecycle of policy & procedures from creation and development to implementation. Includes a sample Business Policy template, sample Business Procedure template, and User Products template. 39 Pages (20-433)

INVENTORY MANAGEMENT PROCEDURE This document establishes a process for the recording, identification, and accountability of all equipment having a predetermined minimum cost. 6 Pages (20-323)

DESKTOP COMPUTING STANDARDS Standard workstation equipment including monitors, keyboard, mice, printers, and software is listed for task-based and fixed function workers. 2 Pages (20-231)

Governance

MICROSOFT TEAMS GOVERNANCE AND POLICY This document establishes standards and guidelines for the use of Microsoft Teams and explains its coexistence with other collaboration technology. 8 Pages (20-1229)

ONEDRIVE FOR BUSINESS GOVERNANCE This document governs the administration, maintenance, and support of the OneDrive for Business tenant. 4 Pages (20-1227)

SHAREPOINT ONLINE GOVERNANCE This document governs the administration, maintenance, and support of a production SharePoint Online tenant as well as the external tenant used for external sharing. 8 Pages (20-1225)

GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE These slides demonstrate governance for executives and security, showing how the environment is controlled. 10 Pages (20-1224)

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

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

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

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)

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

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

HR / Personnel

EMPLOYEE ONBOARDING / OFFBOARDING Described here are procedures for onboarding and offboarding employees using SharePoint, Azure Automation, and PowerShell. 10 Pages (20-1354)

INTERNATIONAL TRAVEL ACCESS POLICY This policy focuses on accessing company resources from international locations. 1 Page (20-1323)

IT ONBOARDING / OFFBOARDING POLICY This policy helps ensure employees are onboarded and offboarded in an accurate and timely manner. 2 Pages (20-1318)

ALTERNATE WORK SCHEDULE The following is a voluntary alternative work schedule template. 4 Pages (20-1097)

FOREIGN TRAVEL STANDARD An organization shares a travel policy that helps prepare for international business travel procedures. 2 Pages (20-867)

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

EMPLOYEE ONBOARDING PROCEDURE The following onboarding packet walks the team through the first day on the job to probationary review. It includes helpful checklists and acknowledgment. 9 Pages (20-638)

OFFBOARDING CHECKLIST Designed for an employer, this checklist example applies when preparing for an employee's departure. 1 Page (20-637)

OVERTIME POLICY This is an example of one company's overtime pay policy, including requirements and eligibility. 1 Page (20-565)

ALTERNATIVE WORK ARRANGEMENTS Alternative work arrangements can reduce traffic congestion during peak periods, reduce commute trips, increase productivity, and/or provide personal benefit to employees to balance work and home life needs. 8 Pages (20-563)

ON-CALL POLICY Procedures for authorizing, assigning, and compensating on-call duty are defined in this policy. 2 Pages (20-562)

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

BUSINESS & TRAVEL EXPENSE POLICY This describes company policy on submission of expenses for reimbursement. 3 Pages (20-466)

TRAVEL POLICY To be used in conjunction with a company travel guideline policy, this policy describes the planning, submission, and approval of travel expenses incurred while traveling on official company business. 10 Pages (20-452)

TRAVEL GUIDELINES The following guidelines are for the planning & approval of travel expenses and to ensure the expenses are appropriately reviewed, approved, and reimbursed. 2 Pages (20-451)

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)

LIFECYCLE MANAGEMENT PROCESS This document includes the lifecycle of policy & procedures from creation and development to implementation. Includes a sample Business Policy template, sample Business Procedure template, and User Products template. 39 Pages (20-433)

POLICY DEVELOPMENT This document takes you through the main steps in policy development, approval, and implementation. 8 Pages (20-432)

CODE OF CONDUCT POLICY Employees will be expected to adhere to the ethical and acceptable standards of conduct set forth in this policy to ensure that the company operates professionally and safely. 6 Pages (20-414)

RESPECTFUL WORKPLACE POLICY This policy is designed to ensure that employees work in a respectful workplace, free of bullying, harassment, discrimination, and violence. 7 Pages (20-398)

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

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

EMPLOYEE TERMINATION POLICY This policy describes termination due to resignation, retirement, job abandonment, or termination. 1 Page (20-228)

VENDOR TRAVEL POLICY This policy applies to all vendors, consultants, and contractors traveling on behalf of the company or its subsidiaries. Vendors are required to comply with this policy when requesting incurred reimbursable travel expenses as permitted by a contract. 1 Page (50-269)

CORPORATE EXPENSE GUIDELINES This document provides guidelines and establishes procedures for all associates incurring out of pocket expenses for the benefit of the company. 11 Pages (50-268)

CORPORATE TRAVEL GUIDELINES This guide gives associates a clear and consistent understanding of expectations and procedures for corporate travel and expenses, while maximizing the company's ability to negotiate discounted rates with preferred suppliers and reduce travel spend. 11 Pages (50-267)

Incident Management

RANSOMHUB RANSOMWARE PRESENTATION This presentation was given during a NOREX session and is published with the author’s permission. 7 Pages (20-1404)

INCIDENT RESPONSE WORKFLOW The workflow pictured is an example of one organization’s incident response process. 1 Page (20-1311)

CONTINGENCY PLANNING PROCEDURE The contingency procedure includes what must be done to recover key hardware components that business software and applications require. 3 Pages (20-1300)

INCIDENT RESPONSE PROCEDURE The incident response defined plan will address the seven stages of incident response: preparation, detection, analysis, containment, eradication, recovery, post-incident activity. 4 Pages (20-1299)

SECURITY INCIDENT RESPONSE POLICY This policy is designed to ensure that computer security incidents are properly identified, contained, investigated, and remedied. 5 Pages (20-1289)

INCIDENT RESPONSE AND BREACH POLICY This policy sets some of the requirements and responsibilities for staff during an incident or breach activity. 5 Pages (20-1201)

INCIDENT RESPONSE PLAN PROCEDURE The following procedure provides clarity on what specific actions are needed and appropriate when dealing with incidents affecting both internal and outsourced systems. 12 Pages (20-1200)

CHANGE MANAGEMENT PROCESS EXAMPLE This guide outlines the resources and process steps required to manage changes to the production environment. 23 Pages (20-1127)

IT SYSTEMS CHANGE MANAGEMENT POLICY This policy governs IT system changes and streamlining processes while mitigating security vulnerabilities and potential loss. 3 Pages (20-1126)

CHANGE MANAGEMENT POLICY This policy describes how to document change management for security and protect information assets and systems from threats. 4 Pages (20-1125)

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

SUPPORT DESK TRIAGE PROCEDURE This document outlines a procedure to establish service expectations and informs employees of the method by which Support Desk requests will be prioritized and what resolution times can be expected when an incident is reported. 3 Pages (20-926)

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

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

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

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

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

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

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

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

Internet / Intranet

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)

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)

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)

Mobile Computing

MOBILE & WIRELESS PROGRAM GUIDE These guidelines describe the expectations and limitations of company-issued mobile phones, personal mobile phones used for work, mobile hotspots, internet sticks, and related options. 3 Pages (20-1324)

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)

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

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)

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

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

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)

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)

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)

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

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)

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)

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)

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)

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)

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)

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)

Network / Remote Access

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)

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

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)

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)

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)

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)

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)

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)

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

Password

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

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

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

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

Physical Access

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)

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

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)

SAMPLE DATA CENTER SOP Standard Operating Procedure for a data center has many variations. Below is a sample SOP. 2 Pages (20-721)

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)

DATA CENTER SECURITY This policy outlines data center rules and procedures. 5 Pages (20-643)

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

Policy Templates

INTERNAL AI POLICY MEMO An example of an internal employee memo explaining the introduction of artificial intelligence governance to enable sharing of information and appropriate safeguards. 1 Page (20-1399)

SOFTWARE VENDOR EVALUATION MATRIX This template provides a process for recording software comparisons. 5 Pages (20-1321)

IT CHANGE MANAGEMENT POLICY This process provides a systematic way of managing changes to core systems in production environments. 8 Pages (20-1142)

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)

POLICY DEVELOPMENT This document takes you through the main steps in policy development, approval, and implementation. 8 Pages (20-432)

TEMPLATE FORMATS Three common templates are displayed in this document, with a definition of each. 3 Pages (20-190)

POLICY TEMPLATE The procedure outlined in this template will guide you in the creation of your own policies. 3 Pages (20-189)

PROCEDURE TEMPLATE Writing a company paper can be simple when following this procedure template. 4 Pages (20-188)

DOCUMENTATION POLICY / PROCEDURE Company policy and procedure for the creation of documents is found here. 14 Pages (20-187)

TECHNOLOGY DIRECTIVE TEMPLATE Following is a template for writing company policies. 2 Pages (20-186)

MASTER DOCUMENT LIST TEMPLATE Company documents and policies might be organized according to subject, department, or other details. A master list can be helpful in making sure things can be found. 10 Pages (20-185)

Records Management

DOCUMENTATION TEMPLATE This template is used as an outline for creating policy and instructional documents. 1 Page (20-1347)

ASSET MANAGEMENT CHEAT SHEET Documents specific to asset management are defined, along with the length of time that these documents are maintained. 5 Pages (20-1221)

DOCUMENT MANAGEMENT SYSTEM GUIDE These use guidelines will assist staff to store, share, and archive documents and records. 2 Pages (20-1220)

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)

DISASTER RECOVERY RECORDS RETENTION This policy provides step-by-step procedures for reducing the risk of service disruption in order to ensure continuity of operations. 2 Pages (20-639)

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

PROTECTED HEALTH INFORMATION DISPOSAL This policy provides guidance as it relates to the appropriate disposal of protected health information and personally identifiable information. 2 Pages (20-157)

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

Security

GenAI CHATBOT USAGE This policy addresses the use of a web-based interface to prompt the chatbot in a conversational manner to find answers to questions or to create or edit written content.4 Pages (20-1398)

GenAI USE POLICY This policy addresses the use of Generative AI for business and outlines use cases and approved GenAI systems. 3 Pages (20-1396)

AI USAGE POLICY Guidelines, restrictions, and best practices for the use of Artificial Intelligence (AI). 2 Pages (20-1391)

AI POLICY This policy establishes the principles and governance structure for the development, adoption, and use of Artificial Intelligence (AI). 2 Pages (20-1389)

AI POLICY AND DISCLOSURE This policy outlines principles and guidelines for using Artificial Intelligence language models and chatbots such as ChatGPT, Bing, and other similar tools. 2 Pages (20-1388)

CYBERSECURITY FRAMEWORKS This presentation given at a NOREX event describes cybersecurity frameworks as a series of documented processes used to define policies and procedures.33 Pages (20-1377)

NIST CYBERSECURITY FRAMEWORK AND BUDGETING This presentation describes the components of NIST cybersecurity framework functions: govern, identify, protect, detect, respond, and recover. 9 Pages (20-1362)

PASSWORD CREATION AND PROTECTION POLICY Standards for creating strong passwords, protection of those passwords, and the frequency of change are established in this policy. 2 Pages (20-1361)

IT SECURITY POLICY This policy establishes a comprehensive plan for the protection of information including computers, software, and networks, as well as any third-party consulting or software providers. 4 Pages (20-1360)

AI USAGE AND VENDOR RESPONSIBILITIES This policy outlines the guidelines and responsibilities associated with the deployment of AI technologies by the organization and its vendors. 3 Pages (20-1359)

GenAI AND LARGE LANGUAGE MODEL POLICY This policy outlines the acceptable use of generative AI and Large Language Model (LLM) tools and technologies. 2 Pages (20-1338)

GENERATIVE AI USE POLICY This policy provides guidance and rules for the responsible use of AI by employees. 1 Page (20-1330)

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)

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

SECURITY AWARENESS TRAINING This policy ensures a basic understanding of information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior. 3 Pages (20-1291)

ARTIFICIAL INTELLIGENCE USE POLICY The following policy outlines options for business use of generative Artificial Intelligence (AI) chatbots such as ChatGPT as well as disciplinary action that may be taken for misuse. 3 Pages (20-1272)

AI ACCEPTABLE USE POLICY This policy outlines the guidelines and regulations for the responsible and ethical use of Artificial Intelligence (AI) systems. 2 Pages (20-1268)

AI ACCEPTABLE USE POLICY LETTER This letter provides an introduction to a corporate policy on the use of Artificial Intelligence in the workplace and can be updated or expanded as needed. 1 Page (20-1266)

CLEAN DESK POLICY This policy ensures that all sensitive and confidential information is properly locked away or disposed of when a workstation is not in use. 1 Page (20-1249)

ELECTRONIC BID & SIGNATURE POLICY This policy describes use of electronic transmission and signatures to send and receive bids, proposals, contracts, and other documents related to the award and administration of contracts. 6 Pages (20-1235)

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)

BUILDING THREAT POLICY This is an example policy in the event a suspicious object is found or there is a threat against the building. 4 Pages (20-1100)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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)

WIRELESS CONFIGURATION POLICY Wireless configuration as it relates to the security management process for Information Technology resources is defined here. 2 Pages (20-399)

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

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

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

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

USER MANAGEMENT POLICY Through the careful and accurate handling and maintenance of user accounts and their associated rights/privileges, the integrity & security of systems and resources in ensured. 2 Pages (20-293)

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)

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

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

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

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

USER MANAGEMENT POLICY The objective of this policy is to ensure the integrity and security of information systems and resources through careful & accurate handling and maintenance. 2 Pages (20-229)

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

ON-PREM APPLICATION RISK ASSESSMENT This assessment for on-prem applications includes business need, intended use, data classification, encryption, and more. 4 Pages (50-444)

MOBILE RISK ASSESSMENT A questionnaire, implementation plan, and risk assessment for mobile applications, including access qualifications and data transfer requirements. 3 Pages (50-443)

CLOUD SECURITY RISK ASSESSMENT Business needs and requirements, questionnaire, implementation details, and recommendations following a Cloud security risk assessment. 5 Pages (50-442)

PREPARING YOUR ORGANIZATION FOR AI Artificial Intelligence is emerging as a significant organizational change agent. This presentation, given at a NOREX event, describes how to prepare your organization for Artificial Intelligence by establishing guidance, mitigating risks, and experimenting safely. 22 Pages (50-435)

GenAI POLICY This policy establishes guidelines for responsible and secure use of Generative Artificial Intelligence (GenAI) systems. 3 Pages (50-432)

ARTIFICIAL INTELLIGENCE POLICY This policy defines both acceptable and prohibited uses of AI to protect company values and mitigate legal and ethical risks. 3 Pages (50-431)

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)

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

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

Social Media

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

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

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

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

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

Software

SOFTWARE REQUEST FORM A software requisition is described with the following screen shots. 2 Pages (20-1337)

ARTIFICIAL INTELLIGENCE TOOL GUIDE These tips and guidelines provide general knowledge on exploring AI tools for business use. 3 Pages (20-1254)

SOFTWARE REQUEST PROCEDURE This Information Security Team procedure defines steps for software approval. 3 Pages (20-997)

SOFTWARE POLICY This directive outlines policy about the authorized and unauthorized use of software on company equipment. 1 Page (20-725)

SOFTWARE ENHANCEMENT REQUEST FORM This workbook provides a procedure for business assessment and requesting software enhancement & workflow builds. 6 Pages (20-676)

SOFTWARE LICENSING POLICY All software installed on company IT resources or systems must be properly licensed and used for business purposes only. 3 Pages (20-635)

FREE & OPEN SOURCE SOFTWARE POLICY This policy is intended to ensure the proper use of free and open source software (FOSS). 4 Pages (20-630)

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)

END-OF-LIFE SOFTWARE PROCESS This document describes the process & procedures around identified end-of-life software installs. 6 Pages (20-026)

APPLICATION ASSESSMENT SUMMARY TEMPLATE This heatmap describes applications, recommendations, costs, and rank. 1 Page (50-422)

APPLICATION INTEGRATION QUESTIONNAIRE This template is used for logging application lifecycles, tech stack currency, annual costs, stability, functionality, security, efficiency, and more. 10 Pages (50-421)

APPLICATION ASSESSMENT REPORT TEMPLATE This template shows the process of documenting an application assessment using a heatmap. 2 Pages (50-420)

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

Storage / Backup

BACKUP AND RESTORATION POLICY This policy provides a means to actively manage risks associated with data loss by defining a sound backup regime for all data services. 6 Pages (20-1283)

BACKUP POLICY. This policy explains a procedure for dataset backup schedules for Windows, Linux, VMDK VMware, Exchange, etc. 3 Pages (20-888)

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

ENTERPRISE DATA BACKUP A procedure for the data backup of Enterprise IT systems. 5 Pages (20-871)

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)

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)

DATA STORAGE STANDARD This storage standard expands on the principles outlined in Data Governance Policy (20-708) as they relate to data management, and provides guidance on the implementation and practical application of data storage solutions. 6 Pages (20-707)

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)

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

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

DATA BACKUP POLICY This policy defines the security management process for information technology resources. 3 Pages (20-401)

ONEDRIVE CLOUD STORAGE POLICY This policy establishes guidelines regarding support and usage of the authorized OneDrive Cloud Storage. 8 Pages (20-230)

CLOUD STORAGE USE This guidance document is a brief overview of the file storage tool Cloud Storage, how it works, and the risks involved. 2 Pages (20-147)

PORTABLE STORAGE POLICY This policy provides guidelines and standards for transporting and temporarily storing corporate data. 3 Pages (10-1762)

Vendor 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)

ITS PROCUREMENT POLICY This policy outlines ownership considerations for the ITS end user hardware assets procured to enable employees to perform their job duties efficiently and effectively. 7 Pages (20-991)

THIRD PARTY VENDOR SECURITY POLICY This policy addresses the high-level requirements for system acquisition, development, and maintenance for third-party vendor-provided information systems. 7 Pages (20-990)

SERVICE AGREEMENT THIRD PARTY POLICY This addendum to a Master Service Agreement provides policy on the use of third party software (freeware, open source) as well as third party deliverables. 3 Pages (20-537)

VENDOR TRAVEL POLICY This policy applies to all vendors, consultants, and contractors traveling on behalf of the company or its subsidiaries. Vendors are required to comply with this policy when requesting incurred reimbursable travel expenses as permitted by a contract. 1 Page (50-269)

Work-From-Home

REMOTE WORK AGREEMENT This agreement template describes requirements and expectations of a remote work environment. 2 Pages (20-1112)

REMOTE WORK POLICY Remote work requirements such as hours, eligibility, approval, and equipment are outlined in this policy. 2 Pages (20-1111)

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

TEMPORARY TELECOMMUTING POLICY This policy outlines provisions and regulations for employees who need to work remotely on a temporary basis. 1 Page (20-985)

TELECOMMUTING AGREEMENT This agreement lists employee and company expectations and provision of equipment for employees working remotely. 3 Pages (20-984)

COLLEGE WORK-FROM-HOME PROCEDURES This document describes procedures for a staggered workforce of college employees working on campus and remotely. 3 Pages (20-967)

SAMPLE TELEWORK POLICY Compensation, supplies, equipment, confidentiality, security, and performance are some of the remote workforce topics covered in this policy. 8 Pages (20-886)

FLEXIBLE WORK POLICY This document will highlight three types of flexible work arrangements. 4 Pages (20-825)

IT TELECOMMUTER NORMS These norms are expectations set for employees in addition to a telecommuting policy. 2 Pages (20-824)

FLEX OR WORK-FROM-HOME PROGRAM This document explains one organization's flexible Work-From-Home (WFH) program, including eligibility and options. 4 Pages (20-814)

TELECOMMUTING POLICY Policy and guidelines of telecommuting describe how to improve staff efficiency without compromising productivity. 7 Pages (20-307)

TELECOMMUTING POLICY OVERVIEW Outlined in this policy are telecommuting expectations, equipment, hours of work, eligibility, and more. 2 Pages (20-306)

IT TELECOMMUTING POLICY This document defines guidelines surrounding telecommuting in the IT department and defines which positions are candidates for an alternate work environment. 3 Pages (20-154)

WORK-FROM-HOME POLICY The Work-From-Home program provides a voluntary work alternative while ensuring it is beneficial to both staff and employer. 4 Pages (50-364)

WORK-FROM-HOME BEST PRACTICES The following guidelines explain how to ensure your home network and computer systems are secure. 1 Page (50-363)

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

FLEXPLACE POLICY Various forms of a successful remote work arrangement are explained and referenced in this policy. 5 Pages (50-306)