**Metropolitan Research and**

**Treatment Kernel Network Diagrams**

Mark White, Rajan Pokharel, Terrica Thomas, Katelyn Piert-Provo

University of North Texas

CSCE 4535: Introduction to Network Administration

Dr. Ervin Frenzel

December 12, 2023

**Table of Contents**

[**Introduction 3**](#_wjksar9lz3td)

[**Network Architecture and Internal Connectivity 6**](#_hb9li6hbem64)

[(Figure 1: North American and European Architecture) 6](#_n9z9u09e0fva)

[Internal Network Structure and System Requirements: Europe (Figure 2.1: European Internal Network System Requirements)(Figure 2.2 : European Internal Network Structure ) 8](#_rowhhngq9qt7)

[(Figure 2.3: European Internal Network Structure Server Rack) 9](#_qsfe2jwr8lwt)

[**Internal Network Structure and System Requirements: North America 11**](#_prdwc5cpf5fs)

[(Figure 3: North America Internal Network Structure) 11](#_4rb802y8jux8)

[(Figure 4: North America Internal Network Structure Server Rack) 12](#_g5tuxbvzs3qw)

[Oracle Database System 15](#_txm5q12gmgmf)

[(Figure 5: Oracle Database Schema - Diagram) 16](#_hbbat69flmfk)

[Conclusion 18](#_jl2x9p50lpbz)

[Works Cited 20](#_75e9wssi89j2)

# 

# Introduction

Metropolitan Research and Treatment Kernel (MRTK) is an international institute dedicated to education, research, and innovation. This policy outlines our commitment to protecting the privacy and confidentiality of all individuals associated with the university, including students, faculty, staff, vendors, contractors, etc. This belief applies to all components of the organization, that’s why we carefully considered the network layout for our multifaceted industry silo.

MRTK deals with data from many different sources some of which are: students, faculty, staff, vendors, contractors, consultants, guests, patients, research participants, educational technologies, and healthcare technologies to name a few. This information needs a way to be stored and later accessed from the same location or across the internet securely. The information we are dealing with is sensitive and across country borders, there are treaties and agreements we must follow to ensure the organization is compliant with local and international laws (sensitive private information (SPI), payment card information (PCI), protected health information (PHI), and personally identifiable information (PII)).

This paper will delve into the intricate details of MRTK University's network infrastructure, focusing on the geographically diverse locations across two continents. We will go into the specifics of network diagrams for both North American (California, Virginia, Ohio) and European (Denmark, Turkey, Bulgaria) campuses while explaining the intricate connections that allow for seamless data flow, communication, and collaboration across borders. There are lots of rules and guidelines that must be upheld when transferring data between regions, especially when these borders are international. Keeping that in mind we at MRTK have made it a priority to ensure that confidentiality, integrity, and availability is not only on our watch list but also keeping sure that our organization's many components are regulated to standards and are compliant to any international treaties that its facilities oversee.

Network security measurements have been accounted for and it is a concern for MRTK to ensure that all the sensitive data we deal with is protected behind encryption systems, firewalls, and other monitoring tools like intrusion detection and protection systems. Because MRTK oversees multiple regions the data privacy laws are different and need to be considered, in this case, MRTK has regions in North America and Europe. While these are the main centers for the organization, it has many sister organizations it is involved with for medical and research purposes, and transferring data between companies needs to be done through encrypted channels and stored in data centers that are being surveilled. The confidentiality and integrity of the data are upheld by making sure that data is not manipulated between transit and at rest.

This continues with the availability of the data across all of the facilities. MRTK is a fast-paced environment dealing with medical, financial, and other intellectual data that can be time-sensitive; it is important that data is available to all its users when it needs to be. This is done by making sure that the network diagrams are properly noted and clearly understandable to our technical information technology and security roles. It is important that the diagrams are followed and the protocols are maintained to ensure that MRTK is compliant with standards to ensure that the reputations of the organizations and all its endpoints are good.

In the situation of a server outage or other regional events, MRTK has made it a priority to account for the unexpected. This means that we have planned on how to handle downtown in server rooms by running a redundant array of independent disks on the server racks and by having redundancy in power. That way if there is any possibility of an outage the drives holding important information can safely continue on another drive. Also if there is a power outage we have accounted for this by having an uninterruptible power supply. It is important that we do not lose any important sensitive or confidential data since it affects many different branches. The data centers are compliant with other regulations such as having security guards present on the site and having physical and biometrics security access into the rooms. This is done so that no one other than the authorized employees and staff associated with MRTK are allowed into these rooms allowing them to tamper with technology and network devices.

Finally, the paper will go over the Oracle database which deals with the logical side of the network infrastructure rather than the physical measurements taken. There are lots of components that the organization deals with and it is important for there to be a central database that allows the many different end-points to communicate and transfer data with confidentiality and integrity.

# Network Architecture and Internal Connectivity

## (Figure 1: North American and European Architecture)

Figure 1 shows the network architecture between MRTK’s North American and European hubs. Each hub has network services such as switches, routers, and firewalls which are represented in this diagram. MRTK Routers provide management for data traffic whereas switches facilitate internal networking, and firewalls secure the network entry and exit points. The network hubs are separate entities that allow network management more specific to its region and compliance with data regulations in that area. A few of MRTK's security protocols include firewalls to prevent system intrusion along with role-based access controls.

MRTK’s Data jurisdiction is stored and processed with regard to local requirements in North American and European regions. Data is also encrypted due to international data transfer, ensuring compliance and safe user data. As labeled in the diagram MRTK has firewalls in both hubs responsible for encrypting and decrypting data coming in and out. Also in the diagram bandwidth specifications are labeled, with switches having 1 Gbps and routers having the higher 10 Gbps bandwidth.

Furthermore, redundancy is important for MRTK network operations maintenance, as seen in the diagram the redundant link allows connectivity between the North American and European hubs

## Internal Network Structure and System Requirements: Europe (Figure 2.1: European Internal Network System Requirements)(Figure 2.2 : European Internal Network Structure )

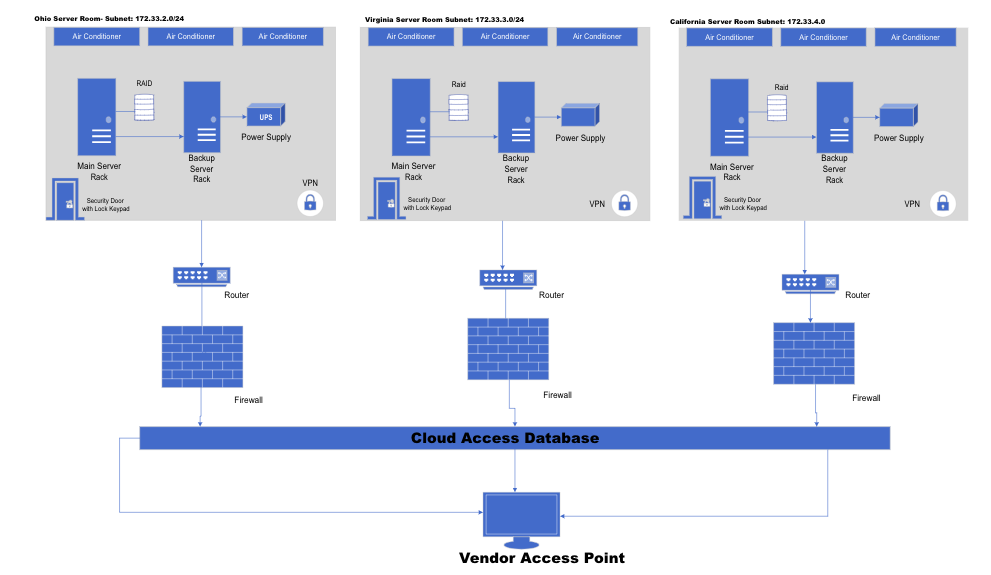
## 

## (Figure 2.3: European Internal Network Structure Server Rack)

The Diagram/Figure 2.1 depicts the internal network structure of our selected sites across three continents. Connectivity for MRTK’s chosen locations: Bulgaria, Turkey & Denmark; requires extreme consideration of many factors. The factors MRTK included were the security of the network, design and the compliance for users. Cloud dumping and third-party vendor access points assure all of these factors. Connecting cloud-based resources to on-premises data centers using site-to-site virtual private networks. Utilizing dedicated network connections to provide high-bandwidth, private connections between cloud providers and on-premises settings. This diagram shows the enabling encryption for every database connection through the routers, both in transit and at rest. This guards against illegal access and safeguards data against interception; installing security groups and firewalls to regulate incoming and outgoing traffic limiting access to the ports and IP ranges that are required. Synchronizing data across continents by using cloud-based data replication services. This guarantees the availability and consistency of data. Mandating that third-party suppliers access databases over secure protocols (such as VPN and SSH).

The server rack—which holds the patch panel, routers, servers, UPS, and monitor—is located in the server room seen in Figure 2.2 & 2.3. The servers are essential for storing data related to MRTK's campus organizations' needs for research, education, and healthcare. In order to guarantee that devices are connected to the internal network without interruption, routers are used to allow data transfer and communication.

# Internal Network Structure and System Requirements: North America

****

# 

## (Figure 3: North America Internal Network Structure)

## 

## (Figure 4: North America Internal Network Structure Server Rack)

Figure 3 shows the internal network for the first continent, North America, which houses 3 campuses in California, Virginia, and Ohio. The diagram includes the server room, the router, and the firewall of each location, as well as the cloud access database and the vendor’ access point.

Beginning with the server room, each location has its own server room. Server rooms are essential as they store the servers, switches, and many other critical equipment. There is a backup server in each server room. This is used to ensure that the data is backed up in case the system fails so the system can continue to operate in case of an incident. According to a paper published by ACM, it is important to have RAID (Redundant Array of Independent Disks) added to each server room to improve data reliability, availability, and performance by mirroring the data from the drive to replace failed drives in case of a failure (Weddle et al., 2007). Next, in the server room are air conditioner systems. These are used to maintain the temperature levels and ensure there is no overheating for the hardware. The UPS cube on the diagram signifies the UPS power supply, which ensures that the system does not experience uninterrupted power. At the door of the server room there is a security door with a biometric scanner. This has been implemented in order to protect all equipment and ensure no unauthorized access.

Specifically in the server room shown in Figure 4 is the server rack in which houses the patch panel, the routers, the servers, UPS, and a monitor. The servers play a critical role in data storage for the purposes of education, research, and healthcare purposes associated with MRTK’s campus organizations. The routers are implemented to facilitate communication and data transfer within the internal network to ensure devices have connectivity seamlessly. There is an Uninterruptible Power Supply to help maintain and protect power disturbance. Lastly, the monitor contains a surveillance camera, which is a combination to review room conditions, access, and security.

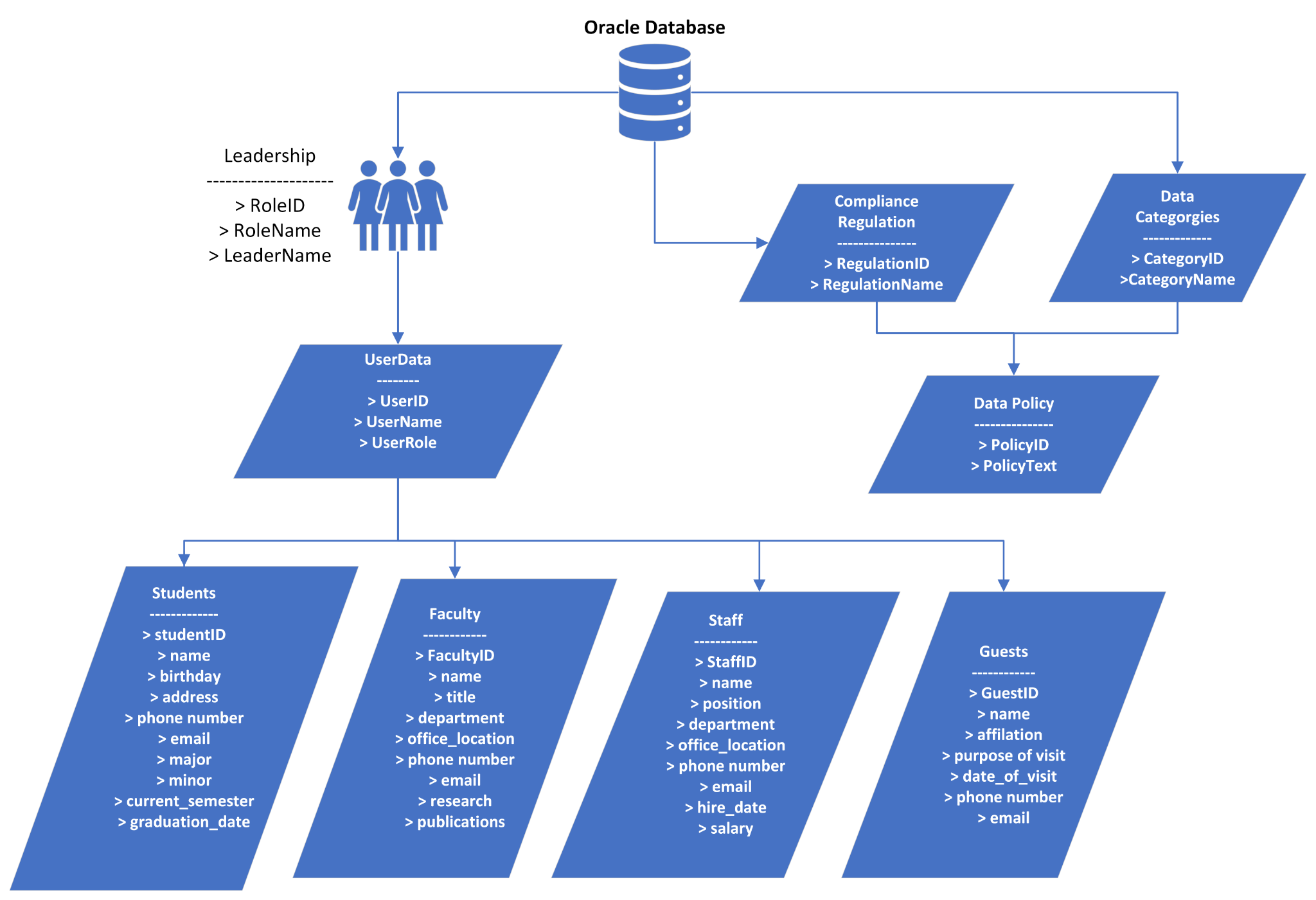
The remainder of the internal network includes a router and firewall that connects to each individual server room, the Cloud Access Database, and a vendor access point. The router assists with connectivity, while the firewall is responsible for safeguarding the network from unauthorized access, cyber threats, as well as, data breaches. As stated in the policy, data is encrypted using SSL/TLS to maintain confidentiality (Policy 2023). The firewalls also control traffic flowing to and from the network to block malicious traffic (Policy 2023). The Cloud Access Database is a centralized cloud-based database that stores the data related to the 3 institutes educational, research, healthcare, and administrative information. The MRTK institution partners with AWS as a cloud service provider. Having a centralized location allows a seamless and convenient location for sharing and retrieving information. Lastly, the Vendor Access Point is used for facilitating access collaboration between the university and external partners, suppliers, and service providers. By having an access point, the MRTK can oversee vendor activity, while also ensuring adherence to privacy and compliance standards in Ohio, Virginia, and California.

# Oracle Database System

MRTK takes data privacy and security very seriously and it is evident through its comprehensive policies and different initiatives. By following legal and ethical standards, the university aims to create a safe and secure environment for all individuals associated with its global operations. This is why we carefully planned out how the database system will be organized to ensure that all boundaries are accounted for and that services are available to all facets.

In order to maintain the organization's data, we need a complex infrastructure built on the Oracle database system for data management, which is an exchange server capable of handling international email communication across all six sites on two continents, VoIP telephony for voice and video calls, and multi-factor authentication for enhanced security. Additionally, the system must comply with the Payment Card Industry (PCI) standards for secure payment processing, and integrate sales, FERPA compliance for student data protection, and a medical component addressing PHI and SBI for healthcare operations. This in depth setup ensures great communication, data security, and compliance with relevant regulations for a large and geographically dispersed organization (Oracle, 2023).

Below is our schema used to create our oracle database and explanation of the relationships between each segment. The database will be compliant with relevant data privacy regulations, such as HIPAA, GDPR, and FERPA. Sensitive data will be encrypted and access will be restricted to authorized users. Finally data will also be backed up regularly and disaster recovery procedures will be in place:



## (Figure 5: Oracle Database Schema - Diagram)

This database has been carefully planned to cover all the compliance check boxes, as well as addressing scalability for future explanations in MRTK. This oracle database can handle larger amounts of data which makes it ideal for an organization like MRTK that has applications and services that have needs that are demanding. While MRTK only deals with North American and European regions, it is able to continue expanding and doing so it can take into account any additional compliance rules and regulations in regards to data privacy and retention laws. The Oracle database offers robust security features, including encryption, access control mechanism, auditing and other tools that allows MRTK to protect the sensitive and valuable information of its users.

Having an approach like this not only safeguards MRTK from legal pressures, but allows the users to be at ease if their personally identifiable information is being held secure and is on the utmost. Oracle database is also known to offer features like data replication, mirroring, and failover mechanisms to ensure high availability and minimal downtime in case of hardware failures or software issues. This is very important for the face-paced environment that MRTK exists in so it is important that availability is present at all times. In the case of unforeseen events like tornados or hurricanes our database enables MRTK to quickly restore their data and systems after a disaster which adds to the physical measures taken in the server room with redundant drives and power.

# Conclusion

The global institute Metropolitan Research and Treatment Kernel (MRTK) is devoted to innovation, research, and education. Our commitment to safeguarding the privacy and confidentiality of all people connected to the university—faculty, staff, vendors, contractors, etc.—is outlined in this policy. While switches enable internal networking and firewalls protect network entrance and exit points, MRTK routers handle data traffic. The network hubs are independent organizations that provide more regionalized network management and adherence to local data laws.

The firewalls in each hub of MRTK, as indicated by the labels in each diagram, are responsible for encrypting and decrypting incoming and outgoing data. This prevents unauthorized access and protects data from interception; security groups and firewalls are installed to control inbound and outbound traffic, restricting access to the necessary ports and IP ranges. Utilizing cloud-based data replication services to synchronize data across continents. The servers are essential for storing data related to MRTK's campus organizations' needs for research, education, and healthcare. The Cloud Access Database, a vendor access point, and a router/firewall that link to each server room make up the remaining portion of the internal network. While the firewall is in charge of protecting the network from cyber threats, unauthorized access, and data breaches, the router helps with connectivity.

In addition, the Oracle database has become known for providing capabilities like data replication, mirroring, and failover methods to guarantee high availability and little downtime in the event of software or hardware malfunctions. This is critical for the fast-paced environment that MRTK operates in, thus availability at all times is crucial. MRTK illustrates the intricate connections that enable smooth data flow, communication, and cross-border collaboration while providing the specifics of network diagrams for campuses in North America (California, Virginia, Ohio) and Europe (Denmark, Turkey, Bulgaria).

# 

# Works Cited

Arseven, M. (2023, May 3). *The Turkish Data Protection Law in 2023: Developments in practice over its seven years - updated edition*. Moroğlu Arseven. https://www.morogluarseven.com/news-and-publications/the-turkish-data-protection-law-in-2023-developments-in-practice-over-its-seven-years-updated-edition/

Bowen, P., Hash, J., & Wilson, M. (2007, March 7). *Information security handbook: A guide for managers*. CSRC. https://csrc.nist.gov/pubs/sp/800/100/upd1/final

Bulgaria, A. U. in B. (2022, August 24). *Privacy notice for international students*. AUBG. https://www.aubg.edu/privacy-notices/privacy-notice-for-international-students/

California, U. (2023). *Research policy analysis and coordination*. UCOP. https://www.ucop.edu/research-policy-analysis-coordination/policies-guidance/record-retention/index.html

Capacity, C. (2023). *Privacy policy*. Copenhagen Capacity. https://www.copcap.com/privacy-policy

Chandramouli, R. (2022, November 17). *Guide to a secure enterprise network landscape*. CSRC. https://csrc.nist.gov/pubs/sp/800/215/final

Department of State, U. S. (2020, January 1). *United States Department of State Treaties in Force*. United States Department of State Website. https://www.state.gov/wp-content/uploads/2020/08/TIF-2020-Full-website-view.pdf

Marron, J. (2022, July 21). *Implementing the health insurance portability and accountability act (HIPAA) security rule: A cybersecurity resource guide*. CSRC. https://csrc.nist.gov/pubs/sp/800/66/r2/ipd

Murray, B. (2023, March 29). *Multi-factor authentication policy*. University Policies. https://policy.uconn.edu/2023/03/29/multifactor-authentication/#:~:text=Multi%2DFactor%20Authentication%20(MFA)%3A,such%20as%20a%20token%20generator

NIST, N. (2018, May 21). *NIST Special Publication 1800-Series General Information*. https://www.nist.gov/itl/publications-0/nist-special-publication-1800-series-general-information

NIST, N. (2021, September 23). *Managing the security of information exchanges: NIST publishes SP 800-47, rev. 1*. https://www.nist.gov/news-events/news/2021/07/managing-security-information-exchanges-nist-publishes-sp-800-47-rev-1#:~:text=NIST%20Special%20Publication%20%28SP%29%20800-47%20Revision%201%2C%20Managing,to%20manage%20the%20protection%20of%20the%20exchanged%20information.

North Texas, U. (2023). *14.003 acceptable use - policy.unt.edu*. UNT. https://policy.unt.edu/sites/default/files/14.003%20Acceptable%20Use\_0.pdf

Nursing Solutions, N. (2023). *2023 NSI National HealthCare Retention & RN Staffing Report*. https://www.nsinursingsolutions.com/Documents/Library/NSI\_National\_Health\_Care\_Retention\_Report.pdf

Oracle. (2023, January 4). How policies work (without identity domains). https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/policies.htm

SANS Institute. (2014, June). *Security policy templates*. Information Security Policy Templates | SANS Institute. https://www.sans.org/information-security-policy/

Science Safety Security, P. H. E. (n.d.). *Science Safety Security – finding the balance together*. ASPR. https://www.phe.gov/s3/law/Pages/International.aspx

Uniform Law Commission, U. (2022). *Uniform commercial code*. Uniform Law Commission. https://www.uniformlaws.org/acts/ucc

United States Code, O. of the L. R. C. (2023). *23 USC 503: Research and technology development and deployment*. https://uscode.house.gov/view.xhtml?req=%28title%3A23%2Bsection%3A503%2Bedition%3Aprelim%29.

Weddle, C., Oldham, M., Qian, J., Wang, A.-I. A., Reiher, P., & Kuenning, G. (2007). Paraid. *ACM Transactions on Storage*, *3*(3), 13. https://doi.org/10.1145/1288783.1289721