Edwin Charlery

Monroe College

22SP-IT373-44 - Network Security

Maureen Monaghan

07/30/2022

Contents

Company of Choice: Jannou Credit Union

Research on company: Jannou Credit Union is a financial institution situated in Castries, St Lucia. Its main focus is to efficiently serve the clientele while incorporating automation and technology to achieve such a goal. Being a financial institution, it is equipped with both the physical means of security as well as technological mean. In terms of physical security, the credit union has implemented surveillance cameras as well as security guards as well as fencing in order to keep the infrastructure secure. The building is also equipped with a fire detection system to instantly alert personnel of any fires within the building. The credit union has also implemented a secure room for the servers which is inaccessible by any unauthorized party. Jannou has incorporated both hardware and software firewall in order to filter incoming and outgoing traffic. The core system is based on windows domain which is responsible for controlling and maintaining user access to files and network drives, while also maintaining user privileges. The Credit Union also uses IP based phones in order to contact one and other and has so vendor software as well as a few custom software integrated in their network. Jannou Credit Union deals with confidential member information and continues to instill confidence in their clientele when it comes to assurance of confidentiality and maintaining the integrity of their information.

Overview:

This security policy has been designed for Jannou Credit Union and focuses on web application security, email security, server security, in addition to those security guidelines, this policy is also focuses on acceptable encryption, end user encryption protection, password guidelines requirements, remote access , wireless technology and standards, database credentials, software installation, technological and equipment disposal.

Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy outlines the requirements for protecting encryption keys that are under the control of end users at Jannou Credit Union. These requirements are designed to prevent unauthorized disclosure and fraudulent use of encryption keys. The protection methods outlined will include operational and technical controls. This policy also enforces best practices for the creation of strong passwords at Jannou Credit Union, such as the use of lengths greater than 8 characters, the use of symbols and techniques such as passphrases. In addition, this policy also provides guidelines for the proper use of Jannou Credit Union’s email system and raises user awareness of what Jannou Credit Union deems as acceptable and unacceptable use of its email system.

This policy further defines rules and requirements for connecting to Jannou Credit Union's network for remote access. These rules and requirements are designed to minimize the potential exposure to Jannou Credit Union from damages. The policy also focuses on ensuring that information systems owned by Jannou Credit Union are secure and protected. Jannou Credit Union provides computer devices, networks, and other electronic information systems to meet

missions, goals, and initiatives. Guidelines are also included in the is policy which devices must satisfy to connect to Jannou Credit Union wireless network infrastructure. Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by an Jannou Credit Union IT Department.

This policy examines the requirements for installation of software on Jannou Credit Union computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within Jannou Credit Union computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

The disposal of technology equipment and components owned by Jannou Credit Union to ensure that data is not captured as well as ensuring that the organization keeps within maintaining an ecofriendly environment is also a crucial component of this policy. Web application assessments will also be performed to identify potential vulnerabilities as a result of inadvertent misconfiguration, weak authentication, insufficient error handling, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of Jannou Credit Union services available both internally and externally as well as satisfy compliance with any relevant policies in place. Effective implementation of this policy will minimize unauthorized access to Jannou Credit Union proprietary information and technology.

Scope

This policy applies to all Jannou Credit Union employees and affiliates. The encryption keys covered by this policy are encryption keys issued by Jannou Credit Union and used in conducting corporate business which will be used to safeguard the credit union’s data. In addition, guidelines are also included which applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins. Emphasis is also placed on the appropriate use of any email sent from a Jannou Credit Union email address and applies to all employees, vendors, and agents operating on behalf of Jannou Credit Union. This policy further examines the use Jannou Credit Union owned workstation used to connect to the Jannou Credit Union's network. This policy applies to remote access connections used to do work on behalf of Jannou Credit Union, including reading or sending email and viewing intranet web resources.

Furthermore, the policy applies to all wireless infrastructure devices that connect to a Jannou Credit Union network or reside on a Jannou Credit Union site that provides wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. Equipment that are no longer needed by the credit union are also examined and provides a detail procedure for the proper practices of disposing or selling old equipment, also all web application security assessments will be performed by Jannou Credit Union.

General

Acceptable Encryption Policy

Algorithm Requirements:

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

Key Agreement and Authentication:

Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

End points must be authenticated prior to the exchange or derivation of session keys.

Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

All servers and applications using SSL or TLS must have the certificates signed Symantec.

Key Generation:

Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

Key generation must be seeded from an industry standard random number generator (RNG).

End User Encryption Key Protection Policy

All encryption keys covered by this policy must be protected in order to prevent unauthorized disclosure and fraudulent use.

Secret Key Encryption Keys:

.Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorized by Jannou Credit Union. If the keys are for the strongest algorithm, then the key must be split, each portion of the key is encrypted with a different key that is the longest key length authorized and then each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.

.Symmetric encryption keys that are not in use must be protected with security measures at least as stringent as the measures used for distribution of that key.

Public Key Encryption Keys:

Public keys are passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it is issued. The private key should only be available to the end user who issued the digital certificate.

Commercial or Outside Organization Public Key Infrastructure (PKI) Keys:

In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user.

Hardware Token Storage:

Hardware tokens storing encryption keys will be treated as sensitive company equipment. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer when not in use. End users traveling with hardware tokens are prohibited from storing or carrying tokens in the same container or bag as any computer.

Personal Identification Numbers (PINs), Passwords and Passphrases:

All PINs, passwords or passphrases used to protect encryption keys must a have minimum length of 8 characters.

Loss and Theft:

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to Jannou Credit Union's IT Department. The systems administrator will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

Password Construction Guidelines

Strong passwords are long, the more characters you have the stronger the password or the more time required to crack the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Passphrases are both easy to remember and type, yet meet the strength requirements, this will surely aid with the retention of password and deter the storing of passwords on paper under keyboards or in easily accessible locations.

Poor, or weak, passwords have the following characteristics and are prohibited from use on the network:

•Contain eight characters or less.

•Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

•Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

•Also “Welcome123” “Password123” “Changeme123”

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of Symantec password vault software that is authorized and provided by Jannou Credit Union. Whenever possible, also enable the use of multi-factor authentication.

Email Policy

.All use of email must be consistent with Jannou Credit Union policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices. Jannou Credit Union email accounts should be used primarily for Jannou Credit Union business-related purposes; personal communication is permitted on a limited basis, but non Jannou Credit Union related commercial uses are prohibited.

.All Jannou Credit Union data contained within an email message or an attachment must be secured according to the Data Protection act of Saint Lucia.

.Email should be retained only if it qualifies as a Jannou Credit Union business record. Email is a Jannou Credit Union business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

.The Jannou Credit Union email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Jannou Credit Union employee should report the matter to their supervisor immediately.

.Users are prohibited from automatically forwarding Jannou Credit Union email to a third party email system without any authorization from the System Administrator. Individual messages which are forwarded by the user must not contain Jannou Credit Union confidential information.

.Users are prohibited from using third-party email systems and storage servers such as Google, and MSN Hotmail etc. to conduct Jannou Credit Union business, to create or memorialize any binding transactions, or to store or retain email on behalf of Jannou Credit Union. Such communications and transactions should be conducted through proper channels using Jannou Credit Union approved documentation.

.Using a reasonable amount of Jannou Credit Union resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. To be specific only the use of educational purposes are prohibited.

.Jannou Credit Union employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

.Jannou Credit Union may monitor messages without prior notice Jannou Credit Union IT Department is not obliged to monitor email messages.

.Clientele information such as financial records shall not be transmitted through emails.

Network Security

Remote Access Policy

.It is the responsibility of Jannou Credit Union's employees, contractors and vendors with remote access privileges to Jannou Credit Union's corporate network to ensure that their remote access connection is given the same consideration as the Jannou Credit Union network or better.

.General access to the Internet for recreational use through the Jannou Credit Union's network is strictly limited to Jannou Credit Union's employees, contractors and vendors. When accessing the Jannou Credit Union's network personal computers are prohibited, and only corporate assigned computers are authorized. Users are responsible for preventing access to any Jannou Credit Union's computer resources or data by non-Authorized Users. Performance of illegal activities through the Jannou Credit Union's network by any user is prohibited. The Authorized User bears responsibility for and consequences of misuse of the authorized user access. Authorized Users will not use Jannou Credit Union's networks to access the Internet for outside business interests.

Requirements:

.Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases.

.Authorized Users shall protect their login and password, even from family members.

.While using a Jannou Credit Union owned computer to remotely connect to Jannou Credit Union's corporate network, authorized Users shall ensure the remote host is not connected to any other network at the same time.

.All hosts that are connected to Jannou Credit Union's internal networks via remote access technologies must use the most up-to-date anti-virus software which will be provided by the IT department (Fortinet fortigate).

Wireless Communication Policy

General Requirements:

All wireless infrastructure devices that reside at Jannou Credit Union site and connect to a Jannou Credit Union network, or provide access to information classified as Jannou Credit Union confidential, or above must:

•Abide by the standards specified in the Wireless Communication Standard.

•Be installed, supported, and maintained by an approved support team.

•Use Jannou Credit Union approved authentication protocols and infrastructure.

•Use Jannou Credit Union approved encryption protocols.

•Maintain a hardware address (MAC address) that can be registered and tracked.

•Not interfere with wireless access deployments maintained by other support organizations.

Wireless Communication Standard Policy

General Requirements:

All wireless infrastructure devices that connect to a Jannou Credit Union's network or provide access to Jannou Credit Union's confidential or restricted information must:

•Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.

•Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.

•All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a Jannou Credit Union's network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

•Enable WiFi Protected Access 2 Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS

•When enabling WPA2-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point

•Disable broadcast of SSID

•Change the default SSID name

•Change the default login and password

Server Security

Database Credentials Coding Policy

General:

In order to maintain the security of Jannou Credit Union’s internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

Specific Requirements:

· Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.

· Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.

· Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.

· Database credentials may not reside in the documents tree of a web server.

· Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.

· Passwords or passphrases used to access a database must adhere to the Password Policy.

Retrieval of Database Usernames and Passwords:

· If stored in a file that is not source code, then database usernames and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the username and password must be released or cleared.

Access to Database Usernames and Passwords:

· Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.

· Developer groups must have a process in place to ensure that database passwords are controlled and changed on a semiannually basis.

Software Installation Policy

•Employees may not install software on Jannou Credit Union computing devices operated within the Jannou Credit Union network.

•Software requests must first be approved by the head of department and then be made to the Information Technology department or Help Desk via the network change request form.

•Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need.

•The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

Server Security Policy

General Requirements:

Approved server configuration guides must be established and maintained by Jannou Credit Union. The following items must be met:

•Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

-Server contact(s) and location, and a backup contact

-Hardware and Operating System/Version

-Main functions and applications

•Information in the corporate enterprise management system must be kept up-to-date.

•Configuration changes for production servers must follow the appropriate change management procedures.

Configuration Requirements:

.Services and applications that will not be used must be disabled where practical.

.Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

.The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

.Do not use a trust relationship when some other method of communication is sufficient.

.Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

.Servers should be physically located in an access-controlled environment.

.Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Monitoring:

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

•All security related logs will be kept online for a minimum of 1 week.

•Daily incremental hard drive backups will be retained for at least 1 month.

•Weekly full hard drive backups of logs will be retained for at least 1 month.

Security-related events will be reported to Jannou Credit Union, who will review logs and report incidents to stake holders. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

•Port-scan attacks

•Evidence of unauthorized access to privileged accounts

•Anomalous occurrences that are not related to specific applications on the host.

Technology Equipment Disposal Policy

Technology Equipment Disposal

.When Technology assets have reached the end of their useful life they should be sent to the Jannou Credit Union IT department for proper disposal.

.The Jannou Credit Union IT department will securely erase all storage mediums in accordance with current industry best practices.

.All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defense standards.

.No computer or technology equipment may be sold to any individual other than through the written-off equipment sales processes identified in this policy.

.All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

.The Jannou Credit Union IT department will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.

.Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed if it cannot be used on existing computing devices.

Employee Purchase of Disposed/written-off Equipment:

.Equipment which is working, but reached the end of its useful life to Jannou Credit Union, will be made available for purchase by employees.

.All equipment will be advertised internally before purchases in order to give everyone a chance to consider acquiring the device. This ensures that all employees are aware of available items.

.The Finance and Information Technology manager will determine an appropriate cost for each item.

.All purchases are final. No warranty or support will be provided with any equipment sold.

.Any equipment not in working order will be donated or disposed of according to current environmental guidelines.

Application Security

Web Application Security Policy

Web applications are subject to security assessments based on the following criteria:

a)New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

b)Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.

c)Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

d)Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

e)Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Systems Administrator.

All security issues that are discovered during assessments must be mitigated based upon the following risk levels:

a)High – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment.

b)Medium – Medium risk issues should be reviewed to determine what is required to mitigate the issue and scheduled resolution process accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues.

c)Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

The following security assessment levels shall be established by Jannou Credit Union.

a)Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities.

b)Quick – A quick assessment will consist of an automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

c)Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

The current approved web application security assessment tools in use which will be used for testing Jannou Credit Union web applications are Acunetix and APIsec

Policy Compliance

Compliance Measurement

The Jannou Credit Union IT Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

.All application releases must pass through the change control process.

.Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Systems Administrator.

. Any program code or application that is found to violate this policy must be remediated within a 60 day period.

Exceptions

Any exception to the policy must be approved by the Jannou Credit Union board of directors in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definition & Terms

1)AES: Advanced Encryption Standard is a symmetric encryption which uses the same key when encrypting and decrypting data. There are three lengths of AES encryption which each provides a different combination of keys which can make the decrypting process more of a challenge for an individual or program. It is currently the industry standard for encrypting wireless connections.

2) Certificate Authority: this is an organization who is responsible for validating the identities of entities and binding them to digital certificates.

3)Digital Certificate: Serves as a cryptographic identity document used as a proof of ownership of a public key.

4)Hash functions: A hash function scrambles data and is then converts that data into numerical values, this algorithm ensures that no matter the input length the output hash value is always the same.

5)LDAP: Lightweight Directory Access Protocol is a protocol for enabling users to locate and access data on an organizations network. It is currently used to provide a central location for authentication.

6) Mac Address: Media Access Control address is a unique identifier for network interfaces, it is also considered to be a burned in address because it is uniquely assigned by the manufacturer and IEEE.

7)Malware: Also known as malicious software which is designed to damage and destroy computers, examples are viruses, trojans, worms, and spyware.

8)Public Key cryptography: is an encryption method that requires the use of both public and private key algorithm also known as asymmetric key cryptography which is used to secure data communications.

9)SSID: Service Set Identifier, this is basically the name of the wireless network. It helps differentiate wireless local area networks from each other.

10) Strong Passwords: is considered to ne a password that is constructed to be difficult for a person or program to predict.

References:

Vulnerability scanning tools. Vulnerability Scanning Tools | OWASP Foundation. (n.d.). Retrieved July 30, 2022, from https://owasp.org/www-community/Vulnerability_Scanning_Tools

Hanna, K. T. (2021, November 19). *What is a strong password?* SearchEnterpriseDesktop. Retrieved July 30, 2022, from https://www.techtarget.com/searchenterprisedesktop/definition/strong-password#:~:text=A%20strong%20password%20is%20one%20that%20is%20designed,defeat%20the%20purpose%20by%20creating%20a%20memorable%20password.

Arthur Cole Arthur Cole is a freelance content creator. He also has a more than 10-year experience in program development for macOS, Cole, A., Approved by Brett Johnson This article has been approved by Brett Johnson, by, A., & Johnson, B. (2020, January 9). *What is a MAC address & what is a MAC address used for*. Data recovery tips. Recover deleted files on Mac, Windows. Retrieved July 30, 2022, from https://www.cleverfiles.com/howto/what-is-mac-address.html

What is AES encryption and how does it work? Cybernews. (2022, April 21). Retrieved July 30, 2022, from https://cybernews.com/resources/what-is-aes-encryption/

What is an SSID? Tutorials Point. (n.d.). Retrieved July 30, 2022, from https://www.tutorialspoint.com/what-is-an-ssid

What is a hash function? definition, usage, and examples. IONOS Digitalguide. (n.d.). Retrieved July 30, 2022, from https://www.ionos.com/digitalguide/server/security/hash-function/

Gillis, A. S. (2019, November 15). *What is LDAP (Lightweight Directory Access Protocol)?* SearchMobileComputing. Retrieved July 30, 2022, from https://www.techtarget.com/searchmobilecomputing/definition/LDAP

Cisco. (2022, June 6). *What is malware? - definition and examples*. Cisco. Retrieved July 30, 2022, from https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

What is Digital Certificate?: Guide on the importance of Digital Certificate. EDUCBA. (2021, August 24). Retrieved July 30, 2022, from https://www.educba.com/what-is-digital-certificate/

Team, S. S. L. S. (2021, December 9). *What is a Certificate Authority (CA)?* SSL.com. Retrieved July 30, 2022, from https://www.ssl.com/faqs/what-is-a-certificate-authority/

What is public key cryptography in information security? Tutorials Point. (n.d.). Retrieved July 30, 2022, from https://www.tutorialspoint.com/what-is-public-key-cryptography-in-information-security

Information security policy templates: Sans institute. Information Security Policy Templates | SANS Institute. (n.d.). Retrieved July 30, 2022, from https://www.sans.org/information-security-policy/