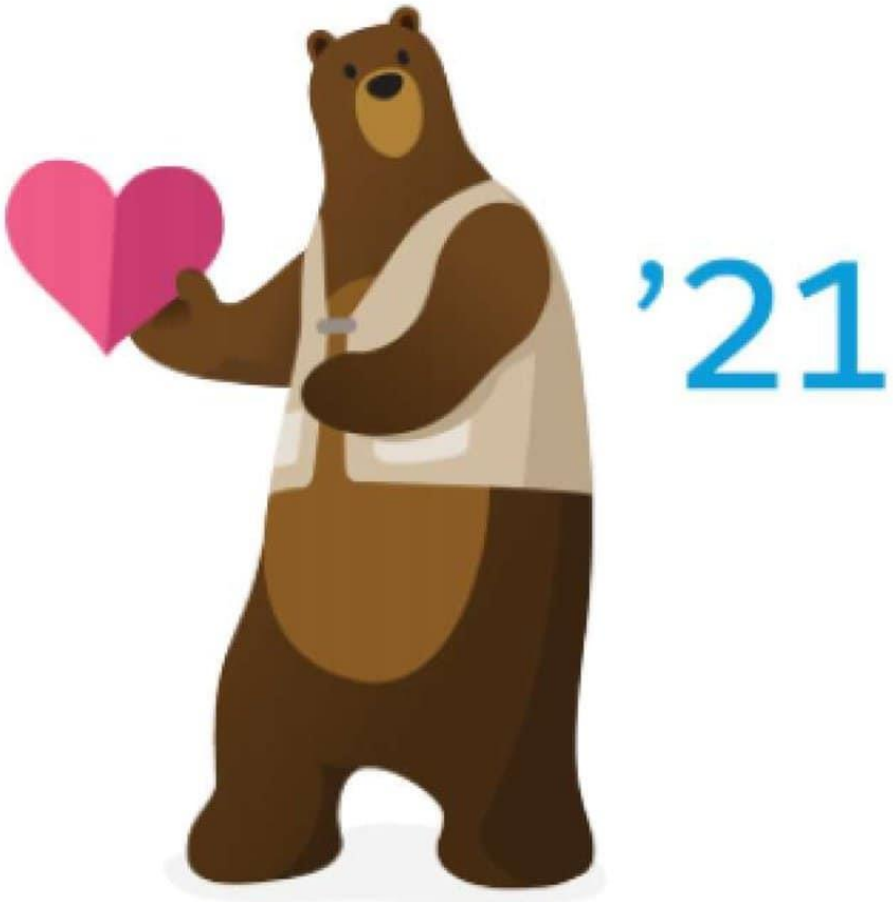
Salesforce Supply Chain Security Memo, Policy & Guidelines



INFORMATION SECURITY POLICIES – PROJECT 2 – TEAM 8

Team Members: [Austin Kent, David Chen, Tanpong Tanthien, Mohammad Zaid Khaishagi]

Salesforce

Cybersecurity Supply Chain

Memorandum

To: Board of Directors, Salesforce
From: Tanpong Tanthien, Security Manager, Salesforce
Date: March 26, 2021
Subject: Proposed cybersecurity supply chain memo, policy and guidelines

Executive Summary

The purpose of this memorandum is to provide the rationale for the proposed Salesforce cybersecurity supply chain policy and guidelines. This recommendation allows Salesforce to implement a proactive set of solutions centered on people, process and technology to prevent and mitigate potential cybersecurity supply chain threats across our suite of products and services. The integrated approach of the policy expands beyond our organization to provide supply chain security best practices for our providers, contractors and customers.

Key Risk and Threats

Technology Risks

Cybersecurity posture of our suppliers can pose a risk to our own organization since any vulnerabilities that threaten our suppliers' systems are also a potential risk to our own system because of our systems' dependence on them. Open source projects also have unique risks such as contributions with malicious code that can compromise our systems. Similarly, foreign sourced software and services have unique risks based on geopolitical climate.

Security of third-party software and services that are incorporated into the development processes of our systems are other sources of supply chain risk, even when the cybersecurity posture of the suppliers is reasonable. Not maintaining or updating the software and services can expose our systems to vulnerabilities and lead to risks that could have been easily avoided.

Changes to software and services made by the supplier can also introduce risk because the new features or the modified parts can potentially have unforeseen interaction with our systems. This can open new vulnerabilities which might not have existed before the changes, modifications or updates.

Customers' risk resulting from our products can also have an effect on our organization. This is because the products we provide can interact with other software and services which can expose vulnerabilities for our consumers' systems. Since such vulnerabilities originate from our products, it can affect our organization and make us liable for them.

Human Risks

One of the biggest causes of security breaches is human error. This error often stems from employees who have not received proper training or education, especially in regards to security, for the job that they are performing. These under-trained employees often fail to implement the correct security measures for their tasks and fall prey to common security attacks.

Process Risks

A major supply chain risk regarding the process of Salesforce product acquisition is verifying third party products. Careful evaluation should be conducted on which products meet security requirements to ensure that SalesForce is not at risk of a data breach. A simple mistake involving our operation processes can be devastating to Salesforce business practices and long-term relations with customers.

Relevant Legal Requirements and Cybersecurity Standards

The proposed changes to the Salesforce supply chain policy take into consideration the following legal requirements, industry standards, and other international regulations.

- ISO-27002: We integrated this standard into our policy because it aligns with internationally recognized security requirements and thus makes collaboration with foreign partners more efficient.
- NIST Risk Management Framework: This policy takes these recommendations into consideration for managing cybersecurity risks.
- PCI-DSS: Salesforce should take PCI-DSS into considerations since it provides products for the financial sector as well.
- HIPAA: Since Salesforce has products for healthcare, this regulation is taken into consideration in the supply chain policies.

Recommendations and Next Steps

Recommendations for Technology

Addressing and analyzing cyber risk to our suppliers is a key part of reducing the risk faced by Salesforce. This involves ensuring that our suppliers propagate the same level of security requirements. It also requires them to have appropriate levels of security in their own internal development processes and procedures such as adhering to the best practices and industry standards for security. These should be enforced for all of our suppliers, including service and software providers, subcontractors, open source projects and foreign sourced software and services.

Ensuring security of software and services addresses any vulnerabilities that might result from using third-party products. This would involve taking the appropriate steps to mitigate any risk from these sources. The measures depend on the type and source of the product, but includes measures such as penetration testing, network access control, audit logs, data backups, isolation or restriction from accessing critical resources, and secure authentication methods.

Regular assessments ensure that our systems are not exposed to risks resulting from any modifications or changes made to our dependencies. **Maintaining and updating** third-party dependencies help mitigate any risks from vulnerabilities that have already been addressed.

Security assurance through audits and certification helps address the downstream cyber supply chain risk. This gives reasonable assurance to our customers about the security practices and measures implemented in the development lifecycle of our products.

Recommendations for People and Knowledge

Salesforce, its suppliers and vendors should work together to create a security minded culture amongst their employees. Such threat sharing culture would provide the whole supply chain system with more awareness on cyber threats. With the correct environment and training, employees can effectively utilize the technological protection provided to them.

Recommendations for Processes and Governance

Business and development processes focused on cyber resilience by design should be taken to ensure that both Salesforce internal product development as well as external business with third party products is secure. Formal procedures such as contractual agreements, checkpoints, and verifications are necessary to reduce errors across the supply chain.

Rationale

Security starts with the employees that make up the organizations. Security minded employees and culture would provide Salesforce, suppliers, and vendors with the ability to connect in a secure way.

After the employees, securing the organization's processes takes precedence. The proposed cyber supply chain policies and guidelines for Salesforce processes and governance limit poor business standards and maintain Salesforce's goal of providing quality assurance of its products.

To ensure security of Salesforce's services, it is important to address the security of the technology leveraged by the organization. Securing the internal development processes of our suppliers along with securing the interaction between third-party software and services with our systems help reduce the supply chain risks. Additionally, performing security assessment of these products regularly further reduces the risk

Salesforce

Cybersecurity Supply Chain

Policy and Guidelines

Overview

In the past decade, digital transformation has forever changed the global supply chain economy. Supply chain is no longer just the flow, movement or delivery of source materials from the supplier to the manufacturer or to the end user. Nowadays, Supply chain is also the exchange of information, technology, and software solutions from one organization to another across the whole supply chain systems. These innovative solutions can range from “complex big data storage, cloud services, e-purchasing, e-sourcing, artificial intelligence to predictive analytics solutions.” [1] The transformation of logistical efficiency to customer relationship management (CRM) services is Salesforce's main product.

Although businesses across the world are embracing digital transformation and rushing to implement technology into their day-to-day business operations to add more value and gain advantage over their competitors, they are leaving themselves vulnerable to supply chain risks that come with digital transformation.

A supply chain attack or third-party attack is when adversaries compromise our systems through outside suppliers or partners with access to our organization's digital assets, such as our networks, software or data. Digital transformation has dramatically evolved the threat landscape of our organization because more vendors and partners are “touching more of our confidential data than ever before.” [2] On the other hand, Salesforce (as one of the world’s leading service providers) is also getting access to more of our customers’ sensitive data along with downstream customers’ data across multiple supply chain systems. “Our organization is only as secure as our weakest link,” [3] so the security of our providers and customers in the supply chain is also our concern. Cyber threat actors can target vulnerabilities in the vendors’ systems and effortlessly infiltrate Salesforce’s network. Hence, it is pivotal that our organization understands these risks as well as take appropriate actions to prevent and mitigate third-party attacks.

Purpose

The purpose of the policy below serves to highlight the risks associated with the “digital transformation of supply chains globally.” [1] The policy serves to provide a well-structured supply chain information risk assessment framework for Salesforce Enterprise, our third-party vendors, business partners, and customers. It also serves to establish the goals and the vision for preventing and mitigating supply chain cyber-attacks. By taking a step-by-step approach to divide the risks into manageable components, this policy presents solutions that align with the Mutually Exclusive and Collectively Exhaustive (MECE) problem solving principle. The policy and guidelines are not “supplier-centric, but scalable and information-driven.” Hence, it can be applied to various issues related to cybersecurity supply chain risks. The policy shall be made easily available at all times to everyone whose duties relate to cybersecurity and privacy. [4]

Scope

“This policy applies to the use of information, software, electronic and computing devices, and network resources to conduct Salesforce business or interact with internal networks and business systems, whether owned or leased by Salesforce, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Salesforce and its subsidiaries along with vendors and customers in the supply chain systems are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Salesforce policies and standards, and local laws and regulation. This policy applies to employees, contractors, consultants, temporaries, and other workers at Salesforce, including customers and all personnel affiliated with third parties.” [4]

The scope of Salesforce Supply Chain Security Policy references and aligns with the Consensus Policy Resource Community by the SANS Institute.

Governing Policy

Salesforce is committed to building and maintaining transitive trust with our third-party partners and customers. An integral part of our mission is our stance on providing successful cybersecurity and privacy programs that ensure data protection for our customers across our products and services. [5]

Salesforce is transforming the future of customer relationship management, and we understand the complexity and risks that comes with that innovation. To mitigate the risks of that transformation, Salesforce has been building resilience by design by enforcing three broad mandates: a) expanding beyond technical solutions to create a well-rounded cybersecurity program that protects the organization; b) ensuring sufficient support and informed decision-making by engaging all stakeholders; and c) integrating information security with corporate tactical and strategic initiatives to foster trust and value creation. [6]

Nevertheless, one type of threat extends beyond our organization's scope of governance — supply chain attack. Supply chain security is a responsibility that must be shared among every company in the supply chain system. The supply chain as a whole is only truly secure when all entities throughout the supply chain "carry out effective, coordinated security measures to ensure the integrity of supply chain data, the safety of products, and the security of the global economy." [3] Because supply chain security is a shared responsibility, Salesforce Enterprise and its third-party vendors shall comply with this policy. Additionally, its customers along with other related companies in the supply chain system should also follow these best practices

"Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem." [1]

To fully understand the supply chain security problem, it is pivotal to assess the risks by traversing the spectrum from people, process to technology. As a result, this governing policy was created and divided into technical policies with solutions that are "mutually exclusive of each other and collectively exhaustive in terms of the whole." [7] There are three main types of

technical policies: a) Technology Policy; b) People and Knowledge Policy; and c) Process and Governance Policy.

The Technology Policy focuses on the technological aspect of addressing compromised software, hardware, networks, data and other digital assets that are shared among our third-party vendors and customers to protect them from cyber attacks and data breaches. This policy is divided into two parts to address various types of technical audiences : a) a central technology policy that can be applied to the general third-party vendors and customers; and b) industry-specific solutions and guidelines for audiences in the healthcare industry and financial sector.

“As supply chains grow in complexity, so does the amount of hands in proximity to the technology that drives supply chain activities.” [1] This translates to an increase in risks associated with human error. The purpose of the People and Knowledge Technical Policy is to ensure alignment in values with the people involved in the supply chain system from Salesforce and its subsidiaries to its vendors and customers. The People and Knowledge Technical Policy is also closely aligned with existing Salesforce Human Resource Policy. Both policies shall be used for assessing and mitigating supply chain security risks caused by people and lack of shared knowledge.

The Process and Governance Technical Policy provides a benchmark for conducting comprehensive assessments and redesigns of Salesforce’s third-party providers and customers related business operational processes to attain the desired level of cybersecurity, privacy, operational efficiency, customer success, service experience and data governance. The policy strives to enhance operational performance and business processes in terms of the three lines of defense internal security controls and supply chain risk management as well as support ongoing change management activities to help redesigned long-term business operations that are sustainable. By providing a framework for designing seamless, structured and secure process flows, the policy helps eliminate vulnerabilities, inefficiencies and redundancies in the current business operations across the supply chain systems. [8]

Because technology will improve cybersecurity only if there are systematic and secure processes that are implemented around it, technology cannot be the solution to any problem by itself. Moreover, “processes are only as good as the people who execute them.” [9] Therefore, using People and Knowledge Policy, Process and Governance Policy and Technology Policy together is a path towards achieving supply chain cybersecurity for organizations and for the global economy.

Technology Policies

Definitions:

Supplier: A third-party who provides either a software or a service which is used by our company. Interchangeably used with providers.

The suppliers may be categorised as vendors or contractors [2]. These are defined as:

- **Vendors:** Those companies whose products in the form of software or services that we make use of in our own internal development processes.
- **Contractors:** Those companies that we hire to perform some specialised task for us. This may be a company such as one that is hired to develop or work on a certain part of our product.

Providers: Those entities which provide their software or services to us, which we make use of in our operational systems. This may include open-source projects, proprietary software, software developed through contractual work, or software/services procured from foreign sources, either corporate, governmental, or both.

Policy 1: Assessment of Suppliers' Cyber Risk [1]

In order to ensure the security of our supply chain, it is essential to make sure that the cybersecurity practices of our providers are of an appropriate level so that the risk of attacks through this approach is reduced as much as possible.

The suppliers must be able to give adequate security assurance regarding their internal cybersecurity procedures and practices.

Since it may be possible to have additional controls implemented for contractors and because the software/service being developed by them would be specific to our needs, additional security requirements must be placed on contractors.

For foreign sourced software/services which we make use of, there is an additional risk that is presented in the form of political pressures and nation-state attacks that may happen through the supply chain. Additional controls and assessments must be made to address this unique risk.

Guidelines:

The points to implement that apply to both vendors and contractors for Assessment of Suppliers' Cyber Risk include the following:

1. **Assess the cyber security posture of the company:** The policies and practices of the company must be evaluated to be of acceptable standards.
2. **Regular security audit of the supplier:** The supplier must undergo a regular security audit which assures that their security posture is of an acceptable level. This audit may be performed by Salseforce or any other reputable auditor or even both, as appropriate.
3. **ISO 27001 and ISO 27002 compliance:** The company should be compliant with ISO 27001 and ISO 27002 standards.
4. **Ensure third-party personnel security [3]:** The company should have proper personnel security measures and practices in place.
5. **Require the company undergo a regular security audit:** The company must have a policy where they regularly undergo a security audit done by a reputable and reliable security auditor and/or an audit done by our own organisation.
6. **Follow NIST Framework:** The company must be following the NIST Cybersecurity Framework and must implement it in their development processes.
7. **Suppliers' supply chain [4]:** Any issues that might arise in the suppliers' own supply chain must be communicated promptly and with the appropriate details, including how it is being resolved.
8. **Addressing common threats:** The providers should have policies and practices in place to protect against common threats, vulnerabilities and exploits. In addition to other sources, these may be referred to from:
    a. NVD
    b. OWASP

9. **Legal and regulatory requirements:** The service provider must meet the same requirements as described in “Policy for supply chain risks to our customers” as applicable.
10. **Propagation of security requirements [4]:** The service provider must provide assurance that they will propagate the security requirement to any other third-parties that they themselves rely on.
11. **Fallback measures:** Ensure that the provider has fallbacks implemented in case any of any major disruption or compromise of their software and services.

The points which are specific to contractors are:

1. **Security team working on-site [6]:** There must be a security team from our own organisation that works on-site with them to ensure the security of the software we use. The main goals for such teams includes monitoring the security procedures and compliance with agreed security requirements, as well as ensuring the general cybersecurity measures are being followed.
2. **Follow the principles for secure systems:** The contractors must be following the design principles for secure systems in their development process. These include:
    a. Economy of mechanism
    b. Complete mediation of authentication and authorization requests
    c. Fail-safe defaults
    d. Ease of use
    e. Separation of privileges
    f. Least common mechanisms
    g. Audit trails
3. **Source code is obtained:** The contractors must make available all source code that is related to the task or the software being developed.
4. **Use of secure tools and technology:** The contractors must not be using tools or technology that is known to be problematic or insecure, or those that have a high likelihood of being so.

Foreign sourced software and services:

Software and services procured from foreign providers must undergo additional scrutiny to ensure integrity of the software and services. This may include, in addition to the generally applicable policies:

1. Assurance against politically motivated attacks.
2. Monitoring of foreign political climate and relations.
3. Monitoring provider's position within the foreign political environment.
4. Review before implementing into our organisation any updates, changes or modifications to software or services being provided.

Policy 2: Providers of third-party software/services

The specific third-party software and services from the providers which Salesforce makes use of must be secured by placing strict security requirements upon them. This includes the security requirements for the development processes used by the provider; the level of security assurance for the product; and security of any data, information or systems made available to the providers.

Guidelines:

Third-party providers of software or services must fulfill the following points:

1. **Support for software and services:** The company must be willing to provide prompt support for any security issues that may arise or come to light.
2. **Disclosure of vulnerabilities:** The company must have a policy whereby they provide prompt information and details regarding any vulnerabilities that are discovered in their products being used by our organisation.
3. **Traceability of critical components [4]:** The critical components of the software and services provided must be traceable and the assurance thereof must be provided by the third-parties. This would allow the tracing of a software/service's full technological stack in the case of an attack.
4. **Managing product lifecycle and availability:** Providers should implement processes and procedures for maintaining availability of products being made use of by our

organisation, as well as managing risk associated with them. This includes notification and procedures for products being discontinued or that are no longer offered, and the risks associated with this.

5. **Data handling:** The data must not be retained by the service provider beyond that required for completion of required tasks and strict controls must be implemented in granting access to the data and should only be granted to the minimum access level needed for performing required tasks.
6. **Acceptable Use:** The data or information made available to the service provider must be made use of only to the extent as agreed and access controls must be implemented as per agreement.
7. **Monitor enforcement of security requirements:** The correct enforcement of the stated and agreed security requirements must be monitored.
8. **Suppliers' supply chain [4]:** Any issues that might arise in the suppliers' own supply chain must be promptly communicated and with the appropriate details, including how it is being resolved.
9. **Notification and Collaboration for Incident Management:** The service provider must promptly notify consumers of any security incidents and must work collaboratively to resolve the incident. This may include review of development process and security processes and procedures in place at the provider's organisation.
10. **Disclosure of new and past incidents:** The provider should provide information about previous security incidents which are relevant as well as any that may happen in the future. This includes information about how those incidents were handled and remediated, and what measures are in place to prevent recurrence.
11. **Common Criterion evaluation:** Any products used by our company should be evaluated according to the Common Criterion as being secure to a reasonable level for the purpose of their use.

Policy 3: Open source software and services

Making use of open source software and services greatly benefits the overall development process. However, it also poses unique risks since the responsibility for the software or service may not rest on any single entity.

Since open source software is not generally developed under strict security controls and practices as might be found at a company, the risks must be mitigated before making use of it. The open source software or services must fulfill the security assessment requirements for vendors and contractors, which are appropriate for open source projects. It must also satisfy additional security assessments which are unique for open source projects.

Guidelines:

The requirements for open source software are:

1. **Thorough penetration testing:** A thorough penetration testing must be done on the open source software before making use of it, in order to identify any vulnerabilities in it.
2. **Must be the latest release:** The software should be the latest stable version in order to not fall victim to issues that were resolved in later releases.
3. **Actively maintained:** The software must be actively maintained and not be an abandoned project.
4. **Available code:** The source code must be available for the software.
5. **Code review:** The code for the software must be analysed from a security perspective and deemed to be reasonably secure before making use of it.
6. **Regular review of software security [6]:** The security of the open source software must be evaluated on a regular basis, preferably on each update, to be of an acceptable level
7. **Managing open source vulnerabilities [6]:** There must be a dedicated team which monitors and deals with vulnerabilities that may arise in open source software.
8. **Recording dependencies [6]:** The various dependencies on open source software must be clearly recorded and documented so that in the case where a major vulnerability is discovered, it can be isolated promptly.

9. **Open Source Security Tools [6]:** Salesforce should make use of Open Source Security Tools which provide integrated DevSecOps.
10. **Analysis of commit histories and contributors:** An analysis must be carried out for the commit history and changelog of an open source software that is maintained by its contributors. The main things that need to be focused on:
    a. Anomalous or suspicious commits made to the software/service.
    b. Cyber risk from contributors for the software/service
11. **Risk Assessment of the tools and technologies:** The tools and technologies that are made use of in the development of the open source project must also undergo a thorough risk assessment using the same points as those for Assessing the Suppliers' Cyber Risk as applicable.

Policy 4: Changes to Supplier Services

It is possible that the products which a supplier is providing our organisation which are used in our development processes undergo some changes, or there is some other change in the relationship. This poses a supply chain risk.

The points which must be considered when there are changes in supplier relationship or a change in the products of either company are [4]:

1. **Changes to supplier agreements:** In case of changes to the agreements, the items for assessing cyber risk must be evaluated again, along with the items for other relevant policies.
2. **Changes made by Salesforce:** In case that Salesforce makes changes to its own products, the cyber risk of suppliers must be re-evaluated to be appropriate to the new environment. These changes include:
    a. Enhancement of current products and services
    b. New products or services
    c. Modification of products or services
    d. Updates to security control in products or services

3. **Changes made by suppliers:** If suppliers make any changes to their own products or services, a reassessment of their cyber risk must be performed to be appropriate to our organisation's requirements. The changes may include:
    a. Changes or enhancement of current products, services or networks
    b. New products or services, or technologies used
    c. Upgrade or adoption of new tools or technologies, or development environments
    d. Change of physical location of service facilities
    e. Change of suppliers or sub-contracting to a new suppliers
    f. Modification of products or services
    g. Updates to security control in products or services

Policy 5: Third-party software and service

The use of third-party software and services in our development environments and processes means that any vulnerabilities in these leads to a risk to our organisation. These must be addressed by implementing security controls inside our organisation for controlling this risk. It must be properly monitored, updated, maintained, isolated and controlled.

Guidelines:

The points to implement for controlling the risk from using third-party software and services are:

1. **Strict control for data handling:** Any data which access is granted must be under strict control,control, making sure that:
    a. Proper audit logs are kept of all access to data, and
    b. Regular backups are made for the data.
2. **Least privilege to perform tasks:** An assessment of the level of access required for performing the required task must be done before assigning an authorisation level to any personnel; and authorisation must be granted solely to those minimum resources necessary for successful completion of designated task.
3. **Description of data access:** A formal description of what information and data are made available to the service provider along with methods of access must be documented and maintained.

4. **Cataloging of critical software and services:** Those software and services that are provided by third-parties and which are critical to our organisation's operations must be clearly documented and the records for this should be maintained.
5. **Patch management and updating [7]:** The third-party software must be updated with the new patch within 30 days of its release. The patches must also be tested by our own organisation before completely upgrading, to be secure to an acceptable level. This may include:
    a. Penetration testing
    b. Behavioural analysis
    c. Malware signatures
    d. Vulnerability scanning
    e. Anti-virus analysis
6. **Intrusion Prevention and Detection Systems (IPS and IDS):** The third-party software and services must have IPS and IDS setup specifically for them. For example, for mail servers, links must be checked whether they are malicious.
7. **Restricted connectivity:** Software and services which need to have network connectivity to the internet are restricted to have access to only a few validated sites for purposes that may include updates and cloud computing or storage. Measures may include:
    a. DNS filtering
    b. Network access control
    c. Misuse detection
    d. Anomaly detection
    e. Firewalls
    f. Whitelisting of websites
    g. Blacklisting of websites
8. **Regular review of logs:** Access logs and audit trails for databases and other critical systems are regularly reviewed for misuse or anomalies in access patterns.
    a. Reviews should be performed every 30 days.
    b. A record of conducted reviews must be maintained for all reviews upto 1 year.

9. **Mapping information flow:** The information made available by or to us should be properly mapped to identify its flow to different entities and third-parties. The entire information flow should be secured.
10. **Change default setting and credentials:** Some products or services may come with preset credentials or other security relevant settings. These must be changed before making use of these products, e.g., router password.
11. **Isolation of third-party products:** The third-party software and services being used must be reasonably isolated from other segments of the development environment. This includes:
    a. Firewalls
    b. Virtualisation
    c. Access control and audit

Policy 6: Downstream Cyber Supply Chain Risk

The risk that is posed to our customers due to any vulnerabilities in our own products also constitutes a cyber supply chain risk to Salesforce. This must also be addressed in order to ensure the integrity of the entire supply chain.

This is addressed by the general cyber security policies implemented in Salesforce for ensuring cybersecurity inside Salesforce. However, additional controls can be placed which provide security assurance regarding minimising cyber supply chain risks to our customers. This takes the form of obtaining security certifications; compliance with various laws and regulation of different jurisdictions, including other countries; and adherence to industry standards for increased security.

Our products must be certified with the appropriate standards and in compliance with the regulations of various countries, sectors and industries, as well as following the industry standards. The points to implement for this are as follows [8]:

1. ISO 27001 and ISO 27002
2. ASP/SaaS

3. C5 (ISAE 3000)
4. CS Gold Mark
5. Disaster Recovery and Business Continuity Plan
6. DoD Impact Level authorisations
7. Third-party security assessment
8. FedRAMP
9. GDPR
10. IRAP
11. HITRUST
12. ISMAP
13. NIST SP 800-171
14. Privacy Mark for Japan
15. Privacy Shield (framework for complying with EU GDPR)
16. Binding Corporate Rules (BCR), company-specific policies approved by European data protection authorities
17. Service Organisation Controls reports issued by AICPA
    a. Type II reports:
        i. Internal controls
        ii. Security, Confidentiality, Integrity, Availability and Privacy controls
    b. Public report
18. TRUSTe certification
    a. APEC Processor Seal
    b. Privacy Verified Seal
19. UK Cyber Essentials Scheme

Policy for healthcare industry:

The products that our company provides which are intended for the healthcare industry must have additional controls, implemented standards and compliance with regulation. These are in addition to the relevant parts of the general policy for providing security assurance for our customers.These are [8]:

1. HIPAA

2. NEN 7510

Policy for financial sector:

The products that our company provides which are intended for the financial sector must have additional controls and regulatory compliance for providing security in this sector. These are [8]:

1. IRS 1075
2. PCI-DSS

People and Knowledge Policies

Policy 1: Raising Questions and Reporting Concerns

- Salesforce and Suppliers and vendors ("SV") must inform their employees of Salesforce security policies and Codes of Conduct and take reasonable measure to ensure that said employees understand the aforementioned policies

Guidelines:

1. Salesforce and SV should provide employees with documents detailing Salesforce security policies and Codes of Conduct
2. Salesforce and SV should provide employees with the Salesforce questions and concerns hotline[1]: (U.S.) **1-866-294-3540** (International) **1-503-726-2414**
    a. Salesforce and SV employees should call Salesforce with regards to any questions on security and ethical policies and report and concerns they may have
    b. Salesforce will safeguard the confidentiality of employees who report concerns to the best of their ability

Policy 2: Authorized Access

- Only authorized personnel should access Salesforce assets and facilities, both physical and digital. Salesforce and SV must take reasonable measures to ensure that proper security measures are in place to ensure such protection.

Guidelines:

1. Salesforce and SV should ensure passwords are sufficiently strong and changed regularly
2. Salesforce and SV can implement dual-factor authentication for an extra layer of security

- Salesforce and SV must ensure proper permissions are in place such that their employees only access and send data which is required for their tasks.

Guidelines:

1. Salesforce and SV should remove permissions from employees who are no longer working on Salesforce related tasks or the company in a reasonable time

- Salesforce and SV must take reasonable means to ensure that employees access confidential Salesforce data with secure devices

Guidelines:

1. Salesforce and SV should ensure that employees are using only company issued equipment with proper security to access confidential Salesforce data
2. Salesforce and SV should take reasonable steps to ensure the safety and security of personal devices used to access confidential Salesforce data if such devices are to be used
3. Proper device security could include but is not limited to[2]:
    a. Firewalls installed and enabled
    b. Antivirus software used and updated regularly for detecting real time threats
    c. Anti-spyware packages if not included in antivirus software
    d. Complex passwords that include combinations of numbers, upper and lowercase letters, and symbols
    e. Data back-ups to rebuild in case of a data breach or loss
    f. Virtualization to run browsers in a safe virtual environment
    g. Connect to secure networks that reasonably prevent infiltration
        i. Networks should have a secure, encrypted setup with a complex password
    h. Two-factor authentication for a second layer of protection
    i. Use encrypted hard drive and USB drives
    j. Use VPN to encrypt web traffic

Policy 3: Protecting Confidential Information

- Salesforce and SV employees must not disclose confidential Salesforce information without express authorization including, but not limited to[1]:

  Guidelines:

  1. Terms and conditions of your agreement with Salesforce
  2. Salesforce business and marketing plans
  3. Salesforce intellectual property (trade secrets, copyrights, patents, trademarks, and other intellectual property) and technical information
  4. Salesforce business processes
  5. Salesforce product plans and designs
  6. Personal employee or contractor information
  7. Any data generated by Salesforce, or received from a third party by Salesforce, that contains or is based upon confidential information

- Salesforce and SV must ensure that employees do not leave confidential Salesforce information in places where they could be exposed unknowingly

  Guidelines:

  1. Salesforce and SV should ensure that employees are placing documents, both physical and digital, in secured locations
  2. Digital documentation should be encrypted, and physical documents should be stored in a location with access only to authorized personnel

- Relevant Salesforce projects and SV must have a DevSecOps team to ensure that cybersecurity personnel are involved in the development process from the very start

  Guidelines:

  1. Relevant security personnel should work with teams throughout the course of the work related to Salesforce to ensure that appropriate security measures are built into the work

2. SV can hire external security teams, if needed, to help in the DevSecOps process
3. DevSecOps should include automation the facilitate the process
    a. Guidance on such automation can be found here:[3] https://itrevolution.com/book/devops-and-audit/

Policy 4: Employee and Related Personnel Training

- Salesforce and SV must ensure training of employees who interact with Salesforce data or products

Guidelines:

1. Salesforce and SV must use adequate numbers of employees who have suitable training, education, skills, and experience required for the activities they are performing related to Salesforce
2. Salesforce and SV should provide employees who interact with Salesforce data or products reasonable training should they require it such that they can perform their job without unreasonable risk to security
3. Salesforce and SV should inform employees of the risks related to third-party plugins and how to mitigate these risks
4. Salesforce and SV should inform employees of the company response for a data breach and what their role is in the response

- Salesforce and SV must take reasonable measures to ensure that employees are properly updating their devices for the latest security protections

Guidelines:

1. Salesforce and SV should clearly communicate to employees the importance of security patches
2. Salesforce and SV should set deadlines for important security patches to ensure that all devices receive the patch in a reasonable amount of time
3. Salesforce and SV should check devices connected to their system to ensure that they have received the latest security patches in a reasonable amount of time

- Conduct social engineering assessments[4]

Guidelines:

1. Salesforce and SV should hire security professionals and test employee responses to, but not limited to:
    a. phishing
    b. baiting
    c. scareware
    d. telephone vishing
2. Salesforce and SV should take all reasonable measures to ensure that the assessment is conducted under a controlled and safe environment
3. Salesforce and SV should follow up with employees right after the assessment to ensure they learn about the risks

Policy 5: Illegal and Improper Conduct

- Salesforce and SV must take all reasonable measures to ensure that their personnel do not engage in inappropriate conduct while performing work for Salesforce. SV will remove and replace personnel who engage in inappropriate conduct upon the reasonable request of Salesforce.

Guidelines:

1. Such inappropriate conduct includes but is not limited to[1]:
    a. SV employees must not give gifts over $150 in value to Salesforce employees nor should Salesforce employees receive such gifts
    b. SV employees must not offer gifts or entertainment to Salesforce employees at any time during a Request for Proposal or other vendor selection process
    c. Salesforce and SV must not give bribes or facilitation payments for work related to Salesforce and ensure their employees do not participate in such behavior

d. Salesforce and SV employees must follow the appropriate laws and regulations governing the actions and services they perform on behalf of Salesforce

Policy 6: Workplace health, safety, and rights

Workplace culture, environment and safety play a large part in how much employees care about the company and thus the safety of the work they are performing. If employees can not concentrate on their work, they can not implement proper security measures. Studies show that careless and irresponsible employees are a large portion of security incidents.[5][6]

- Salesforce and SV must provide workers with a safe and healthy workplace that complies with all applicable health and safety regulations.

  Guidelines:

  1. Salesforce and SV must take proactive measures to ensure to prevent workplace hazards
  2. Salesforce and SV must not tolerate any threats or acts of violence

- Salesforce and SV must respect individual rights, personal dignity, and privacy while working with Salesforce [1]

  Guidelines:

  1. Salesforce and SV should follow all applicable laws and regulations regarding child labor
  2. Salesforce and SV should respect employees' rights to freely associate and bargain collectively in accordance with all applicable laws and regulations
  3. Salesforce and SV should allow all employees to leave their employment freely upon reasonable notice and never use forced or involuntary labor
  4. Salesforce and SV must compensate employees fairly and follow local wage regulations or collective agreements

    a. If not such regulations or agreements exist, Salesforce and SV should provide employees with reasonable compensation such that they can meet basic needs
5. Salesforce and SV should ensure that working hours and overtime do not exceed applicable legal limits and norms
6. Salesforce and SV should ensure fair and proper hiring, firing, and evaluation processes

Policy 7: Third Parties

- SV should ensure that they inform Salesforce and obtain their permission before giving any data relating to Salesforce to a third party or contracting out any work that will be delivered to Salesforce. They will also ensure that the third party is informed of and understands Salesforce's security policies.

Guidelines:

1. SV should provide Salesforce contact numbers to third-parties hired to do work on or related to Salesforce data and communicate to them Salesforce security policies
2. SV should perform a background check on third-party employees and businesses to ensure they meet reasonable standards for safety and security

Policy 8: Contingency Plan(s)

- Salesforce and SV must have a plan of action on what to do if Salesforce data is leaked or is suspected to be leaked [7]

Guidelines:

1. Salesforce and SV should have pre-approved drafted templates for communicating to stakeholders and employees the optimal message at the correct time
2. Salesforce and SV should ensure that people in various departments know how and what to communicate

3. Salesforce and SV should ensure that all team members and leaders are comfortable talking about any error they may have made

Processes and Governance Policies

This document outlines the Salesforce supply chain cybersecurity policy and guidelines which is under the governance of the Chief Information Security Officer (CISO) who is hereby tasked with ensuring reliability, accuracy, and secure accessibility of Salesforce product data. These policies and guidelines are maintained on the Salesforce website and are fully visible to customers, third party vendors, and any Salesforce employee.

Policies will be clearly integrated into a Data Communication Plan that governs Salesforce, the customers and the third-party vendors. The plan has a blueprint for where data is stored, filed, the period of retention, and how data flows through the supply chain [1].

Policy 1: Security Checkpoint Processes

Product cycle checks are performed at each critical step throughout the entire supply chain from top to bottom. These checks ensure that our products development is repeatable and measurable to mitigate any vulnerabilities thus increasing product resiliency [2].

Guidelines:

Every customer application must integrate security checkpoints throughout the supply chain that will preemptively stop cyber security threats [3]. High overview of processes for security checkpoints that must be integrated into the DevSecOps Lifecycle for the products includes, but are not limited to:

1. Inception Phase: Threat modeling and security as a quality attribute process checkpoint [4].
2. Project Configuration Phase: Securing and hardening environment process checkpoint [4].
3. Code Review Phase: Security focused code review process checkpoint [4].
4. Continuous Integration / Testing Phase: Process checkpoint for Automated Security Testing (Static Analysis, etc.) [4].
5. Quality Assurance (QA) Testing Phase: More Security Testing Process Checkpoint (Penetration Testing, Fuzz Testing, etc.) [4].

6. Transitioning Phase: Security reviews and Acceptance Testing Process [4].

Policy 2: Periodic Audits

Independent auditors will check for compliance to Salesforce cybersecurity policies [2]. The scope includes both internal software developers and external third party vendors or suppliers [3]. Internal control, monitoring and auditing will support and help Salesforce meet regulatory compliance.

Guidelines:

1. Comply to all the Generally Accepted Accounting Principles (GAAP) when it comes to auditing.
2. Must comply with the Sarbanes-Oxley Act Section 404.
3. Perform audits quarterly
4. Publish audit findings and require responses with clear actions within thirty days.
5. Target a due date for each and every gap with a reasonable timeframe
6. In the case of a third party vendor, if gaps are not appropriately closed relations may be discontinued.

Policy 3: International Security Certifications

To ensure that data integrity is maintained and that customer data privacy is secure. Adherence to global standards will aid in stabilizing security by providing quality assurance for internal and external software vendors [5].

Guidelines:

International standards will be one of Salesforces most important aspects of business transactions. Salesforce will implement ISO standards with flexibility from a cybersecurity perspective by obtaining proper certifications and be used as a reference point to how information security should be handled [2] . The relevant components of ISO will be utilized in an agile manner [6]. At a minimum each third party vendor is required to abide to the certifications as outlined by Salesforce. Additional global certifications for trustworthiness to

abide by are the U.S. Federal Information Process Standard (FIPS), IPv6 certification, and the U.S. Department of Defense Unified Capabilities Approved Products List (UC APL) [2].

Policy 4: Validation of Third Party Suppliers

Rigorous reviews will be conducted on potential third party vendors to verify that vendors use reliable processes in adherence to secure transference of data [6]. As part of this review, Salesforce will look at third party vendors documented policies, guidelines, and protocols to check for compatibility and fit.

Guidelines:

Before implementing any new service a third party supplier must be validated before accessing Salesforce systems and data [7]. One criteria for the evaluation is to check that the third party vendors have processes in place to remain agile to changing environments in the supply chains [7]. Every third party vendor will have a performance scorecard with key metrics that measure the amount of data threats that have occurred over a period of time. Another example of a metric is the responsiveness to a threat to Salesforce data. External reviews for a potential third party vendor must be researched extensively before starting a new relationship.

Policy 5: Product Acquisition Process

When possible, Salesforce should purchase a product directly from the third party vendor. Direct purchasing will reduce the risk of counterfeit products. To counteract the possibility of a faulty product merging with Salesforce software, an assessment of customer and company reviews of third-party products is required to prevent a heightened risk of data breach. In the event that a product is relatively new and does not have any prior reviews available, then the Salesforce Technology task force will test the product against the Salesforces' Quality Assurance Framework. "It is often the case that poorly manufactured or designed products will eventually be pushed out of the market", thus, SalesForce shall avoid testing the product first [8].

Guidelines:

Before making the decision to acquire a new product, a formal testing and acquisition process must be followed as defined in the Quality Assurance Framework. For new products that may be

acquired from third party vendors, Salesforce will perform QAF testing to validate if the product meets security requirements. Prior to signing a contract with a third party vendor, the identified security requirements must be defined in the standard contract language - refer to Policy 9 Contractual Agreements. If the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls must be reconsidered prior to purchasing the product [9]. Refer to Policy 8 Risk Register and Policy 9 Contractual Agreements.

The Salesforce technology team will test the product against the Quality Assurance Framework in a separate sandbox environment to protect the integrity of Salesforce's information systems. The software will be run and tested to verify it meets the security requirements and is a legitimate product. Refer to the Technology policies and guidelines for the pertinent processes for modifying purchased software.

Policy 6: Data Access Verification

Sensitive information will be protected and guarded through a Data Access request process [5]. Data Access requests for sensitive information will require a higher level of approval that must be evaluated by a Data Access Review Board. This process will limit access and verify that there is a business purpose for accessing the sensitive data. Once a Data Access request is approved, additional safeguards beyond passwords including [10]. two factor verification will be implemented. In the case of a password leak two factor verification will ensure that only Salesforce employees have access to company data.

Guidelines:

Before data can be accessed, the third party vendor must submit a Data Access request. This request must specify the business need and will be submitted for review and approval before access is granted. The Data Access Review Board will evaluate each Data Access request from a third party vendor before sensitive information is made accessible. If the business needs to access the data is warranted, then the request will be approved and access will be granted. If a Data Access request is rejected by the board, the third party vendor will be notified of the rationale. All open source developers must be required to have strong passwords for accounts

[4]. Additionally passwords will be changed periodically to avoid Salesforce data becoming public domain. Decisions on who will be able to access Salesforce data will be determined by business needs and "third party vendors being appropriately certified in their field of operation" [11]. Business relationships will be strengthened by taking the steps to verify legitimacy of associates in the marketplace.

Policy 7: Detection and Response

In the event of a supply chain cyber security threat has been detected there is a clear plan that defines each step in response to the threat. The objective is to provide quick, effective, and orderly responses to information security matters [3]. For example one step is to notify the Chief Security Information Officer (CISO).

Guidelines:

Every cyber security threat will follow this protocol:

1. Immediate action must take place
2. Notify customers impacted by breach in a timely manner [6].
3. Notify starting with the Chief Security Information Officer of Salesforce and the entire supply chain involved
4. Log the threat into the Detection and Response system
5. Secure systems to ensure system continuity. In case of cyberattacks such as phishing and malware the supply chain members must disable Salesforce software until the attack is cleared, install security updates, increase firewalls, disable remote access, and change passwords on all systems.
6. Conduct a thorough investigation and correct problem
7. Manage public relations for all supply chain members
8. Address legal and regulatory requirements
9. In addition to preventing the intensity of a future threat make sure software is up to date with latest updates to stay ahead of risks and keep caches clean on all devices.
10. Review the situation and determine if a cyber risk should be added to the risk register to monitor and mitigate to prevent recurrences.

Policy 8: Risk Register

Manage a comprehensive list of potential risks with clear mitigation plans for each component of the supply chain. The scope of the risks will cover both Salesforce as well as customer software applications. Furthermore third party vendors must share their own risk registers with Salesforce for transparency and a trusted relationship [10].

Guidelines:

A Customer Cybersecurity survey must be conducted annually. The survey will be sent to all customers of the supply chain [12]. The Salesforce Customer Relationship team will send reminders to maximize the response rate of surveys received. The survey feedback information will be closely evaluated to look for trends, new developments, and ongoing issues that require mitigation to prevent re-occurrence. The survey process will foster continuous and innovative improvements in cybersecurity.

Policy 9: Contractual Agreements

A contractual agreement is required for every customer and third party relationship. Standard contractual language has been established for all agreements with third party vendors and customers that clearly delineates liabilities and accountability in the case of a cyber threat. The agreements cover a variety of different types of potential security data breaches. The intent is to clearly explain the limits of liability of each party.

Guidelines:

Written contracts between customers and third party vendors are required to be drawn up to clearly outline the access and use guidelines, so as to appropriately allocate liability in the case of a breach. The Salesforce Legal team will review and approve every contractual agreement prior to signature.

The Salesforce Contractual agreement template must be used as a starting point.
Standard contract language must include the following at a minimum:

- Quality assurance and Risk sharing clauses [13].

- Stronger contractual language to address the risk for the products that may not fully satisfy our security requirements and controls
- Safeguards that will prevent further losses to customers and the supply chain as a whole In the event that a third party vendor goes out of business
- Remediation language to address third party vendors who are not providing accurate responses in the case of a data breach.

The design and comprehensiveness of each contract will pertain to the level of risk and the nature of the relationship [13]. An overarching master scope of work contract will be developed for long, established third party relationships; each additional new portion of work will be governed by the master scope of work contract. This will save time and effort while still protecting the interests of Salesforce.

Policy 10: Cybersecurity Insurance Process

Insurance will be purchased and secured to protect Salesforce in their relationships with third party vendors. Insurance will provide the coverage necessary to address damages in the case of a cybersecurity data breach. The coverage will be specific to cybersecurity and shall encompass the risks caused by significant disruptions in the supply chain [14].

Guidelines:

Salesforce will employ insurance professionals to identify the level of coverage needed to prevail and mitigate the financial burdens of a significant cyber disruption [15]. An insurance professional will explain what is covered and what is not. The consultation will allow Salesforce to determine the appropriate coverage. Typical supply chain coverage is the minimum requirements. Additional coverage to consider includes contingent business interruption which covers costs associated with a property loss at a third party's business location [14].

For the financial risk not covered by insurance, Salesforce will include contractual terms (refer to Policy 9 Contractual Agreements) and define the risks to monitor and mitigate in the Risk Register (refer to Policy 8 Risk Register).

Bibliography

Memorandum References

[1] "Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC", *CDC*. [Online]. Available: https://www.cdc.gov/phlp/publications/topic/hipaa.html. [Accessed: 30-Mar-2021].

Overview, Purpose, Scope and Governing Policy

[1] "The Cyber Security of Supply Chains: Who's the real risk, Man or Machine?", *Medium*, 2017. [Online]. Available: https://kodiakrating.medium.com/the-cyber-security-of-supply-chains-whos-the-real-risk-man-or-machine-ecdcc365d49d. [Accessed: 17- Mar- 2021].

[2] M. Korolov, "What is a supply chain attack? Why to be wary of third-party providers", *CSO Online*, 2021. [Online]. Available: https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html. [Accessed: 19- Mar- 2021].

[3] N. Lord, "Supply Chain Cybersecurity: Experts on How to Mitigate Third Party Risk", *Digital Guardian*, 2020. [Online]. Available: https://digitalguardian.com/blog/supply-chain-cybersecurity. [Accessed: 30- Mar- 2021].

[4] "Information Security Policy Templates | SANS Institute", *Sans.org*, 2021. [Online]. Available: https://www.sans.org/information-security-policy/. [Accessed: 17- Mar- 2021].

[5] "SalesForce," 15 March 2021. [Online]. Available: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/salesforce-security-privacy-and-architecture.pdf.

[6] "Perspectives on transforming cybersecurity", 2021. [Online]. Available: https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx. [Accessed: 21- Mar- 2021].

[7] “What is the MECE Principle? Understanding Mutually Exclusive, Collectively Exhaustive - StrategyU", *StrategyU*, 2021. [Online]. Available: https://strategyu.co/wtf-is-mece-mutually-exclusive-collectively-exhaustive/#:~:text=First%2C%20%E2%80%9Cmutually%20exclusive%E2%80%9D%20is,occur%20at%20the%20same%20time.&text=When%20applied%20to%20information%2C%20mutually,inclusive%20of%20all%20possible%20options. [Accessed: 18- Mar- 2021].

[8] "Risk Consulting", *KPMG*, 2021. [Online]. Available: https://home.kpmg/sg/en/home/services/advisory/risk-consulting.html. [Accessed: 23- Mar- 2021].

[9] H. Dolfing, "People, Process, Technology (In Exactly That Order!)", *Henricodolfing.com*, 2021. [Online]. Available: https://www.henricodolfing.com/2020/05/people-process-technology-in-exactly.html. [Accessed: 25- Mar- 2021].

Technology Policy References

[1] "Cybersecurity Threat Prevention and Response", *Salesforce.* [Online]. Available: https://trailhead.salesforce.com/en/content/learn/modules/cybersecurity-threat-prevention-and-response/secure-your-supply-chain. [Accessed: 30-Mar-2021].

[2] Assuming that Salesforce makes use of both types of third-parties

[3] "NIST Risk Management Framework | CSRC", *NIST*, 2020. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/800-53. [Accessed: 30-Mar-2021].

[4] "International Standard ISO/IEC 27002", 2013. [Online]. Available: https://gatech.instructure.com/courses/173394/files/folder/Projects/Project%202?preview=20530653. [Accessed: 30-Mar-2021].

[5] "Best Practices in Cyber Supply Chain Risk Management", *NIST*. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf. [Accessed: 30-Mar-2021].

[6] "A Guide To Open Source Security", *Contrast Security*. [Online]. Available: https://www.contrastsecurity.com/knowledge-hub/glossary/open-source-security-guide. [Accessed: 30-Mar-2021].

[7] "Patch Management | Cyber Security | Georgia Institute of Technology", *Georgia Institute of Technology*. [Online]. Available: https://security.gatech.edu/patch-management. [Accessed: 30-Mar-2021].

[8] "Certifications | Salesforce Compliance", *Salesforce*. [Online]. Available: https://compliance.salesforce.com/. [Accessed: 30-Mar-2021].

People and Knowledge Policy References

[1] Salesforce, “GLOBAL SUPPLIER CODE OF CONDUCT.” Salesforce, 2015.

[2] M. Freedman, “18 Ways to Secure Your SMB's Devices and Network,” Business News Daily, 13-Oct-2020. [Online]. Available: https://www.businessnewsdaily.com/11213-secure-computer-from-hackers.html. [Accessed: 29-Mar-2021].

[3] “What is DevSecOps?,” Red Hat. [Online]. Available: https://www.redhat.com/en/topics/devops/what-is-devsecops. [Accessed: 29-Mar-2021].

[4] RSI Security, “How to Conduct a Social Engineering Assessment,” RSI Security, 27-Oct-2020. [Online]. Available: https://blog.rsisecurity.com/how-to-conduct-a-social-engineering-assessment/. [Accessed: 29-Mar-2021].

[5] Achilles, “The effect of 'human factors' in Supply Chain Management,” Achilles, 07-Feb-2020. [Online]. Available: https://www.achilles.com/industry-insights/the-effect-of-human-factors-in-supply-chain-management/. [Accessed: 29-Mar-2021].

[6] “The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within,” Kaspersky Daily. [Online]. Available: https://www.kaspersky.com/blog/the-human-factor-in-it-security/. [Accessed: 29-Mar-2021].

[7] Y. Beck, CISSP, and T. Sconzo, “DATA BREACH ACTION PLAN,” The Jabian Journal, 27-Nov-2019. [Online]. Available: https://journal.jabian.com/data-breach-action-plan/. [Accessed: 29-Mar-2021].

Process and Governance Policy References

[1] Blue Stones Supply Chain, 7 April 2020. [Online]. Available: https://bluestones-sc.co.uk/policies/data-retention-policy/. [Accessed 28 March 2021].

[2] J. N. Stewart, "Perspective: Not all Vendors and Products are Created Equal," *Georgetown Journal of International Affairs*, pp. 91-98, 2012.

[3] "International Standard ISO/IEC 27002," 1 October 2013. [Online]. Available: https://gatech.instructure.com/courses/173394/files/folder/Projects/Project%202?preview=20530653. [Accessed 24 March 2021].

[4] H. Yasar, "Multi Security Checkpoints on DevOps Platform," SlideShare, 21 November 2016. [Online]. Available: https://www.slideshare.net/SonatypeCorp/multi-security-checkpoints-on-devops-platform. [Accessed March 2021].

[5] L. A. Gordon, M. P. Loeb and W. Lucyshyn, "Cybersecurity Investments in the Private Sector: The Role of Governments," *Georgetown Journal of International Affairs,* pp. 79-88, 2014.

[6] "SalesForce," 15 March 2021. [Online]. Available: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/salesforce-security-privacy-and-architecture.pdf.

[7] T. Sobb, B. Turnbull and N. Moustafa, "Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions," *Electronics,* vol. 9, no. 11, 2020.

[8] "Top Threats That Require Third-Party Risk Management," RSI Security, 7 September 2020. [Online]. Available: https://blog.rsisecurity.com/top-threats-that-require-third-party-risk-management/.

[9] D. M. D. Christoffer Karsberg, Security Guide for ICT Procurement ICT Procurement Security Guide for Electronic Communications Service Providers, European Union Agency for Network and Information Security, 2014.

[10] J. Weir and K. Yates, "Supply Chain Collaboration: THE BEST DEFENSE Against Cyber Crime," *Defense Transportation Journal,* vol. 72, no. 4, pp. 15-18, 2016.

[11] "OCC," 30 October 2013. [Online]. Available: https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

[12] M. Korolov, "CSO Online," 4th February 2021. [Online]. Available: https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html. [Accessed 2021].

[13] A. Ghosh and J. Fedorowicz, "Business Process Management Journal," 25 July 2008. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/14637150810888019/full/html.

[14] "Cyber Risk And The Evolution Of Supply Chains," *Aspen Insurance*, 2021.

[15] T. Logan, "The Time for Cyber Insurance:Coverage Improves Supply Chain Resiliency," 2 September 2020. [Online]. Available: https://www.fdd.org/wp-content/uploads/2020/08/fdd-memo-the-time-for-cyber-insurance-coverage-improves-supply-chain-resiliency-rapporteur-summary.pdf.