Privacy Policy for SpaceX

Anil Erturk

[erturkanil@cityuniversity.edu](mailto:erturkanil@cityuniversity.edu)

Kimyou By

[bykimyou@cityuniversity.edu](mailto:bykimyou@cityuniversity.edu)

Kory Skarbek

[skarbekkory@cityuniversity.edu](mailto:skarbekkory@cityuniversity.edu)

Team 8, CS520 Ethical, Legal, and Societal Security

Master of Science in Computer Science

City University of Seattle

**Abstract**

The privacy policy of a company needs to cover confidential data of customers (SpaceX, 2021) (Starlink, 2021), employees (Vengattil, M., Roulette, J., 2020), and the company itself (Ismail, N., 2018). Rockets are considered a military technology, and there are extra laws concerning the data privacy of arms manufacturers. These companies are subject to extra laws talked about in the paper. These laws are aimed at keeping sensitive information hidden. It is common in the rocket industry for clients to request extra privacy (Shacklett, M., n.d). This is mostly a case for government satellites (Thompson, A., 2020). Needing extra privacy for the employee data is also mostly a case for certain government agencies and projects. A notable example of this would-be Sergei Korolev who was the Chief Designer of the Soviet space program (ESA, 2007). Confidential information in the arms industry is taken so seriously that Turkey was kicked out of the F-35 program for purchasing Russian S-400 air-defense systems (Reuters, 2019). This paper talks about the common and unique privacy policy challenges of a rocket company called SpaceX. It also talks about policy and process changes to accommodate work from home and ensure data privacy.

**Keywords:** privacy policy, data privacy, confidential data, rocket industry, arms industry, spacex

**1. Introduction**

Privacy Policies help to understand how organizations gather and handle data. In 2018 the European Union passed the General Data Protection Regulation (GDPR) to help its citizens have better control over their data. The United States on the other hand does not have federal laws protecting consumer data. However, this has not prevented organizations within the United States from implementing their own privacy policies. Having a privacy policy is especially important for organizations that operate in highly regulated industries, such as the aerospace industry. When Coronavirus Disease 2019 (COVID-19) started to spread throughout the world in 2020, many organizations had to adjust how and where their employees were working. This led many people to adjust their working location from the traditional office to working from home. This means more information that used to circulate inside an organization now circulates between remote employees and the organization. This raised concerns over data privacy. The confidential data can be about employees, the customers, and the organization and its products. However, people have been using the internet for a long time and working remotely for a long time. So, this is not a new condition. The technology to deal with data privacy had already existed. It is just a matter of putting that technology and education in place.

**2. Privacy Policy**

To secure the privacy of data while working from home, the first thing that needs to be done is stopping the use of insecure programs. SpaceX and NASA banned their employees from using video conferencing app Zoom, citing “significant privacy and security concerns,” days after U.S. law enforcement warned users about the security of the app and told the users not to make meetings on the site public or share links widely. Coronavirus caused many people to work from home and use new apps that were not as popular before. This opened new attack surfaces that were not as popular before. Trying to keep their employees and their data safe is one of the unique challenges facing aerospace manufacturers since the technologies they develop are considered military technologies and there are special laws concerning the sharing of military technologies. SpaceX suggested email, text, or phone as alternate means of communication. The Intercept reported that Zoom video is not end-to-end encrypted which means the company could view sessions. The company Zoom later “apologized for incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption” (Vengattil, M., Roulette, J., 2020).

Data protection plays a significant role in “preventing data exfiltration, mitigating the effects of exfiltrated data, and ensuring the privacy and integrity of sensitive information” (National Institute of Standards and Technology & U.S. Resilience Project, 2020). This involves using the confidentiality, integrity, and availability triad model to identify and approach sensitive information, operating security practice measures, applying security measures or procedures to any device that will be actively used for business objectives, preventing access to unknown devices. Data protection can be safeguarded within SpaceX by setting encryption keys and integrity controls, using secure implementation to transfer data, and scanning systems frequently to ensure that risks are taken care of.

**Confidential Information**

Other than the employee, customer, and company information that all companies need to keep private, aerospace companies also have other challenges.

It is common in military companies and government agencies to have secrecy behind people, missions, and products. Identities of astronauts and other personnel are sometimes needed to be kept secret. This requires more security than normal contracts to keep employee information private. There are examples of this from multiple countries. Soviet Russia kept the identity of Sergei Korolev a secret. He was the man responsible for the first human spaceflight (Pearlman R. Z., 2011).

A more recent example of extra confidentiality about data of employees is China keeping their astronauts secret but getting them leaked because of blunder. (ESA, 2007)

An example of secret aerospace employees in the USA is operation paperclip where German engineers were brought to the USA after WW2. Because of the national security value of the space program, the identities of the employees were kept secret to protect them. (NASA, 2017)

In the aerospace industry, some of the customers request extra privacy for the payload, mission, contents, capabilities, and orbit. One example of that was payload for the National Reconnaissance Office (NRO), the government agency that oversees the country’s fleet of spy satellites. (Thompson, A., 2020) Since aerospace technologies are considered military technologies, they are bound by extra laws such as ITAR and EAR. ITAR control the export and import of defense-related articles and services on the United States Munitions List (USML). The goal of the legislation is to control access to specific types of technology and their associated data. Overall, the government is attempting to prevent the disclosure or transfer of sensitive information to a foreign national. Specifically, ITAR [22 CFR 120-130] covers the military technologies and space-related technologies. Some of the best practices to secure ITAR data are:

* Build and maintain a secure network by installing and maintaining firewall configuration to protect data and avoiding the use of vendor-supplied passwords and other security defaults
* Assign a unique ID to each person with computer access
* Regularly test security systems and processes
* Protect sensitive data with encryption
* Regularly monitor and test networks
* Implement strong access control measures
* Track and monitor all access to network resources and sensitive data

In SpaceX's work environment, confidentiality plays a significant role to ensure and protect the necessary information of the company, customers, and employees. Also, confidentiality helps to keep secret information from being misused or wrongly disclosed. In addition, to prevent any cybersecurity attack that might affect the confidentiality of the company and business operation, it is then necessary that SpaceX have some way to manage potential risks to the company including the way to investigate cybersecurity incident and the way to prevent leaked information from being posted on public websites. In accordance with (Matousek, 2020), Business Insider stated that SpaceX “company data had been accessed or stolen in a criminal cybersecurity incident; however, business is operating normally while the company investigates the incident.”

**Security Awareness Training**

With the ever-changing work environment, it is extremely important that all employees are up to date with the most recent security policies within the organization. One of the biggest information security weaknesses any organization has is its employees. It only takes one employee making a critical mistake to allow an attacker access to an organization’s network. One of the best ways to make sure employees understand the risks and their responsibilities is to enforce security awareness training. A high-quality security awareness program can help employees recognize and prevent a breach from happening. It helps employees understand the seriousness and importance of information security and the cost it can have on an organization like SpaceX. The more informed employees are about the threats, risks, and how to recognize them the less likely employees are to make a costly mistake. In 2015, the research found that there were more breaches caused by human error than any other factor (Osborne, 2018).

Any security awareness program needs to be up to date. If an organization wants to help prevent a larger forgetting curve, employees need to be reminded of what they may have forgotten. When it has been a long time since someone has done a specific task, it is easy for them to forget the proper way to do it. This means keeping consistent security awareness training helps an organization be preventative instead of reactionary. It is also important for employees to understand the purpose behind the training, and that security awareness training does not just happen when something goes wrong. You want them to understand that security awareness training is something that does not stop just because there have not been any security incidents (Roper et al., 2006).

A model for security awareness is the TEAM model. TEAM stands for training, education, awareness, and motivation. Each of these plays a key role in a proper security awareness program. Training looks to teach employees what they may not know how to do or what they should do. This helps make sure they have the proper knowledge and skills to perform their task in a secure way. Education is to help educate them on what they may not understand, such as the policies, purposes, and reasoning behind the security measures that are in place. Awareness focuses on teaching them what they may not think about. This helps train them to think of things from a security perspective. Motivation is all about motivating the employees to put their training, education, and awareness to work when it counts. This is about performing a task in the proper way that it has been taught (Roper et al., 2006).

|  |  |
| --- | --- |
| **People will not do...** | **So we do...** |
| What they don’t know they should do or don’t know how to do | Training |
| What they don’t think makes sense | Education |
| What they never think of doing | Awareness |
| What they have not reason to do | Motivation |

(Roper et al., 2006)

**Access SpaceX Technology Resources**

To ensure all data remains private at all times, data should be encrypted not only when data is at rest but especially when data is in transit. Data should never be stored on employees' personal devices or even on devices provided by SpaceX when it can be avoided. If data must be stored on a remote device, the device will be provided by the company and secured with top-of-the-line encryption and malware protection software. When connecting to the SpaceX network, employees working remotely must access the network through an approved VPN service. Employees are to avoid using an unsecured network when connecting to the SpaceX network or when using a company-owned device. Employees will also be required to use multi-factor authentication before they are able to gain access to the network (Vanderzanden & Bennett, 2020).

In addition to that, all communication and data exchange between employees should be encrypted to prevent a leak of sensitive information. For example, when connecting to the SpaceX network environment, all communication between ground stations, data centers, and satellites should be secured via encrypted connections like public-key encryption and secure sockets layer which are commonly used for encryption on the network.

Figure 1. Network Communications



(Moss, 2020)

On top of that, to restrict unauthorized access to SpaceX network resources. The firewall should be implemented to help block unwanted files that try to breach the company network. In addition, the firewall also keeps protecting from malicious attacks that pose cyber threats to company network resources. So far “this is one of the latest best practices adopted by several companies. It provides a second line of defense and keeps suspicious external network traffic away” (Tarcomnicu, 2017) Besides firewall defense, the company should use Wi-Fi Protected Access for its network communication, such as WPA2, WPA3 that equipped with Advanced Encryption Standard technology. This Wi-Fi Protected Access has several types of encryption that help to increase network security.

Additionally, to prevent unauthorized access to SpaceX networks, it is important to create the inventory and control of hardware assets that are responsible for regulating all devices on the network. This is the process that allows authorized users access while preventing unauthorized users from gaining access. The inventory and control of hardware assets will manage both the public and the private network aspects of the SpaceX company. Pertaining to every device on the network there will be information listed as to which user the device belongs to, the department they work in, and the address of the network. This will help when it comes to authentication processes, inventory updates, system backups, certifications necessary based on users’ duties, and pinpointing devices that have been exposed to an attack, incident response, and recovery processes.

Besides, to secure accesses and data of SpaceX networks, implementing limitation and control of network ports that are responsible for regulating the ongoing operational use of ports, protocols, and services on networked devices to minimize windows of vulnerability (National Institute of Standards and Technology (NIST) & U.S. Resilience Project). This would involve putting up firewalls, operating multiple machines for different purposes, verifying connections, applying port filtering tools on end systems with a default-deny rule that eliminates any prohibited traffic, keeping the network up to date, and getting rid of any unnecessary old clutter.

**3. Remote Work Policy**

With increasingly more employees working remotely, it has become extremely important for organizations to consider how their privacy policy changes for employees working in these various locations. An organization like SpaceX has less control when employees work outside of the office. Therefore, it is as important as ever to make sure employees are following all policies when connecting to SpaceX’s network or using SpaceX resources. Because of this management of SpaceX needs to not only make sure the privacy policy is up to date but also that employees are familiar with expectations and rules they should be following.

**Remote Access**

Employees should be cautious where they are working remotely from. Not only do employees need to ensure they are connecting to the organization’s network through a secured connection but also that they are aware of who may be viewing or accesses data the employee has access to. Employees should be ensuring they are employing proper physical security techniques as well are digital ones. If a device with sensitive information on it is lost or stolen, there is a chance data can be breached. Again, employees should not store organizational data outside of the organization's network. Employees are expected to take precautions to prevent the theft or loss of the organization’s device(s). Employees should never walk away from a device without locking the screen first and if the employee is in a public setting, should never let the device out of their sight. It is also the responsibility of the employee to make sure all SpaceX devices are secured within the employees' place of residence (Vanderzanden & Bennett, 2020).

**Risk Management for Remote Work**

Nowadays, since the impact of pandemic, most organizations depend on some form of information systems to remotely carry out their daily business interactions. These information systems can include remote works; for instance, data transmissions, office networks, financial networks, or specialized systems (NIST, 2012). While these systems are necessary to the organization’s workflow, but these systems also contain an amount of risk whether these risks involve leaked data or direct damage to the system all involve either directly or indirectly and a monetary loss to the company involved. It is then necessary that SpaceX has some way to organize potential risks to the company including what damages are possible, what the damage amount will be, and how likely the damage will occur.

Risk assessments exist to identify all potential risks to SpaceX and estimate how damaging and how likely each risk is. By utilizing this assessment, SpaceX can prepare for any worst-case or even more common-case scenario and mitigate damages done. Risk assessments can also be used to weigh and approximate the amount of net-gain the company will receive under defined circumstances.

Privacy risk management involves all aspects of an organization and helps employees better understand the tools that they are using, and the risks associated with those tools. Doing a privacy risk assessment is just a part of the overall risk assessment. The purpose of privacy risk assessment is to be able to weigh the risks of data processing and figure out how to best mitigate that risk. When assessing the privacy risk there are options for an organization to consider. The one thing that an organization cannot do is to eliminate the risk. An organization can look to mitigate the risk by putting in place controls and policies to try to limit the risk as much as they can. Another option is to transfer the risk by hiring a third-party to help share the risk. If an organization decides the risk is not worth the benefit, the organization can avoid the risk by stopping the data processing. Last, the organization can just accept the risk if the organization determines that the chance of the risk happening is incredibly low or that the benefit of the data process far outweighs the risk. All privacy risk that an organization faces should be accessed and follow into one of these four categories (NIST, 2020)

**4. Conclusion**

Privacy policies provide employees, customers, and the organization with information on how data is handled. When the Coronavirus pandemic stuck the world, organizations were forced to adjust where and how they employee performed their work tasks. This led to many employees working remotely, specifically from their own personal residences. Although employees working remotely was not a completely new idea, there were new challenges that had to be confronted. Organizations working in highly regulated industries had to be even more cautious about how their employees handled data. An organization like SpaceX had to make sure data used by their employees did not become more susceptible to data breaches. This meant making sure employees were not using software that was not as secure as SpaceX needed them to be.

SpaceX operates in the aerospace industry and operates with various levels of government clearance. Data, such as astronaut's personal information needs to remain secret. SpaceX is also restricted by laws and regulations, such as ITAR and EAR, other organizations are not. These laws and regulations deal with protecting the data the organization has. SpaceX needs to make sure to always protect the confidentiality of its data from security breaches.

It is extremely important the employees have proper security awareness training. Without proper security awareness training, SpaceX would be at an increased risk of an employee error that led to a data breach. Human error is one of the leading causes of security breaches for organizations. Putting in place a security awareness training program that uses the TEAM model can help to increase employee competence in not just following proper procedures but also recognizing a potential security risk and help to prevent a data breach. Some of these potential breaches can also be prevented by have proper procedures in place when accessing or handling data. Making sure encryption best practices are always using on data. Employees should also know how and when to connect to SpaceX’s network. It is also important to understand the importance of protecting company equipment.

Making sure all this security in place is even more important with employees working remotely. SpaceX has less control over how and where employees are using their devices or data. Risk management can help SpaceX better understand the risks they face and help to make sure they have the proper controls in place to help control that risk as much as possible. Although they can never fully eliminate risk, they can mitigate it.

**5. References**

Vengattil, M., Roulette, J. (2020). Elon Musk’s SpaceX bans Zoom over privacy concerns –memo. <https://www.reuters.com/article/us-spacex-zoom-video-commn/elon-musks-spacex-bans-zoom-over-privacy-concerns-memo-idUSKBN21J71H>

Reuters. (2019). U.S. removing Turkey from F-35 program after its Russian missile defense purchase. <https://www.reuters.com/article/us-usa-turkey-security-f35/u-s-removing-turkey-from-f-35-program-after-its-russian-missile-defense-purchase-idUSKCN1UC2GL>

ESA (2007). Sergei Korolev: Father of the Soviet Union’s success in space. <https://www.esa.int/About_Us/ESA_history/50_years_of_humans_in_space/Sergei_Korolev_Father_of_the_Soviet_Union_s_success_in_space>

Pearlman R. Z. (2011). Names of China's Secret Astronauts Revealed by Autographed Envelope. <https://www.space.com/13853-china-secret-astronaut-names-revealed.html>

NASA (2017). Biography of Wernher Von Braun <https://www.nasa.gov/centers/marshall/history/vonbraun/bio.html>

Thompson, A. (2020). SpaceX launches classified US spy satellite, sticks rocket landing to cap record year.   
<https://www.space.com/spacex-launches-nrol-108-spy-satellite-lands-rocket>

Groot J. D. (2020). What is ITAR Compliance? 2020 ITAR Regulations, Fines, Certifications & More  
<https://digitalguardian.com/blog/what-itar-compliance>

SpaceX. (2021). SpaceX Website Privacy Policy. <https://www.spacex.com/media/privacy_policy_spacex.pdf>

Starlink. (2021). Starlink Privacy Policy.

<https://www.starlink.com/legal/privacy-policy>

Shacklett, M. (n.d). How to create a privacy policy that protects your company and your customers. TechRepublic. <https://www.techrepublic.com/article/how-to-create-a-privacy-policy-that-protects-your-company-and-your-customers/>

Ismail, N. (2018). Top tips for protecting crucial data in the manufacturing industry. InformationAge. <https://www.information-age.com/data-protection-manufacturing-industry-123473380/>

Vanderzanden, D., Bennett, R. (2020). Cybersecurity and Privacy: 10 Best Practices When Working From Home. <https://ogletree.com/insights/cybersecurity-and-privacy-10-best-practices-when-working-from-home/>

Tarcomnicu, F. (2017). 5 Fundamental Best Practices for Enterprise Security. <https://www.entrepreneur.com/article/281042>

Osborne, B. (2018). 10 Benefits of Security Awareness Training. <https://resources.infosecinstitute.com/10-benefits-of-security-awareness-training/>

National Institute of Standards and Technology (NIST), & U.S. Resilience Project. (n.d.). Boeing and Exostar Cyber Security Supply Chain Risk Management.   
<https://www.nist.gov/document/nistusrp-boeing-exostar-case-studypdf>

National Institute of Standards and Technology (NIST). (2020). NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>

NIST. (2012, September). NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.

Matousek, M. (2020, March 2). Confidential Tesla and SpaceX documents were leaked online after one of their suppliers was hacked. BusinessInsider.  
<https://www.businessinsider.com/tesla-spacex-documents-leaked-online-after-supplier-hacked-2020-3>

Roper, C., Grau, J., & Fischer, L. (2006). Security education, awareness, and training: from theory to practice. Elsevier Butterworth-Heinemann.

Moss, S. (2020, October 21). Microsoft Azure Space teams up with SpaceX's Starlink and SES's O3b. (Onlinepicture). *Datacenterdynamics*.   
<https://media.datacenterdynamics.com/media/images/MicrosoftSpacePlans.original.jpg>