**SilverCorp Weekly: August 10, 2021**

To all employees:

We here at SilverCorp have to be diligent and practice safe work habits. SIlvercorp communication devices are to be used for work related activities only. Whether it is sensitive email communications or work-related activities. We are going to implement weekly security updates to all company phones, notebooks, and desktop computers. A SilverCorp newsletter will be sent out weekly to keep you informed of all company wide policy updates or changes; including any cyber threats. SilverCorp will also be implementing our “Best Security Practices Courses” on the 1st of every three months. All cyber threat courses will be mandatory with testing.

Note: To mitigate the security risks to Silvercorp. No personal communications devices will be allowed to be used or kept on company grounds. Due to increasing cybersecurity threats that have emerged in the last 2 weeks. Administrative action will be taken for any company violations. Depending on the severity of the infraction. Disciplinary action will be enforced up to termination.

Our research has found SilverCorp is always at potential security risk. Not only from personal communication devices, but also from SilverCorp communication devices.There is plenty we could do to help harden, secure our data, and devices. We all have to work together as a whole. One loose link could bring our company down for weeks or to close SiverCorp indefinitely. Here is food for thought; “The most malicious cyber security threats of 2021**.”**

[**https://www.acronis.com/en-us/articles/malicious-cyber-threats-2020/?gclid=CjwKCAjwx8iIBhBwEiwA2quaq50G5dTPLSiFzBj-oqnkNRf9FCH-W9sdiEJQP7dz\_zYZSKSKofVeIxoC\_boQAvD\_BwE**](https://www.acronis.com/en-us/articles/malicious-cyber-threats-2020/?gclid=CjwKCAjwx8iIBhBwEiwA2quaq50G5dTPLSiFzBj-oqnkNRf9FCH-W9sdiEJQP7dz_zYZSKSKofVeIxoC_boQAvD_BwE)

If you have any further questions or concerns. Get together with your department head and or Cybersecurity Threat Management Team as soon as possible.

Sincerely,

Jose M. Dorado CEO

**Step1: Measure and Set Goals**

**1. Three potential security risks examples that can be carried out if allowing SilverCorp employees to access work information on their personal devices:**

* Not using a password manager or two factor authentication leaves a device vulnerable. If safely practiced this will help harden the device's protection.
* If not always patching and updating the devices software. This could lead to; breaches, theft, ransomware, and destruction of data.
* If the device is lost or stolen, and it is not set for remote data-wipe or lock, it could lead to dangerous consequences for data compromises.

**2. From the above scenario, the preferred SilverCorp employee behavior should be as follows:**

If you are in communications and are off of SiverCorp property on a business trip. You will be using the best security practice of using a secure line of communication. Here are a few examples to help mitigate safe practices and how we can practice them. We have concluded that this would be the best security practice for Silvercorp.

**SilverCorp Best Security Practices for Mobile Devices**

* Use secure connection such as a VPN and do not use public Wi-Fi
* Do not open and block suspicious Email
* Turn on Two Factor Authentication
* Update and Patch the OS and Apps when available
* Do not download or run unauthorized Programs or Apps
* Always Lock your device and use a Password Manager
* Use cloud security and back up frequently
* Remote Lock and Data Wipe if lost or stolen
* Let Management and Security advisors know if anything suspicious comes up

[**https://solutionsreview.com/mobile-device-management/7-essential-mobile-security-best-practices-for-businesses/**](https://solutionsreview.com/mobile-device-management/7-essential-mobile-security-best-practices-for-businesses/)

**3. SilverCorp methods to measure how often employees are currently not behaving according to preferred behavior?**

* Logging on and off devices will be logged and monitored daily
* Weekly newsletters of policy changes and security threats will be sent out
* Semi-Annual cybersecurity threat trainings will be mandatory with testing
* False positive emails and attachments will be sent out randomly to employees from our Cyber Threat Management Team
* Administrative infractions will be monitored and dealt with immediately

**4. Our goal here at SilverCorp to reach regarding your behavior as an employee is as follows.**

* The actions and behaviors as an employee shall be minimized and maintained to a minimum for Cyber threats
* 38% of employees that work outside of the workplace will tighten and minimize their exposure to cyber threats to a 2%
* 68% of employees in the workplace will reduce their risk to cyber threats to 1%
* Their will be a 100% up tick in cybersecurity training and behaviour enforcement

**Step 2: Involving the Right People**

**At SilverCorp everyone has to be involved. This job is everyones from the CEO to the newest trainee. Five employees that need to be involved are:**

1. The Chief Executive Officer (CEO)

* He will have to look over and sign off on all policy changes and implementation of those changes.The CEO reports to all board members.

1. The Chief Financial Officer (CFO)

* The CFO charts and monitors the company's financial trajectory. He helps ensure the company uses its finances wisely.

1. The Chief Operating Officer (COO)

* Ensures a business is able to function effectively day-to-day. Typically reports directly to the CEO.

1. The Chief Information Security Officer (CISO)

* Manages risk to an organization's data throughout its lifecycle. They help develop security policies and procedures.

1. The Chief Information Officer (CIO)

* Develops IT systems that support the business. Typically reports to the CEO.

<https://uclavirtlacyb-bjb7417.slack.com/files/U0285LW9CUD/F029Z45E5D0/2.1_introduction_to_security_within_the_organization.pdf>

**Step 3: Training Plan**

**How will SilverCorp train all employees on this security concern?**

1. The training will be a combination of both online and in person. It will be semi-annual for the testing. The format will always finish in an online quiz and or exam with random generated phishing email. They will be updated on what is happening out in the wild and the frequency of cyber attacks.

**What topics will be taught and practiced?**

**The example of topics will be:**

1. Phishing email attacks
2. Use secure connection such as a VPN and do not use public Wi-Fi
3. Do not open and block suspicious Email
4. Turn on Two Factor Authentication
5. Update and Patch the OS and Apps when available
6. Do not download or run unauthorized Programs or Apps
7. Always Lock your device and use a Password Manager
8. Use cloud security and back up frequently
9. Remote Lock and Data Wipe if lost or stolen
10. Letting Management and Security advisors know when anything suspicious comes up

**How will the SilverCorp measure the training and its effectiveness?**

* We will monitor and document all training effectiveness by changing up the format frequently to freshen the course subjects. Determining how the employees are scoring will determine how much we should change up the tests. Course effectiveness is key to the security of SilverCorp.

**Bonus: Other Solutions**

**Training alone often isn't the entire solution to a security concern. Two other potential solutions can be:**

1. **SilverCorp will use infractions as Administrative control.**

* The goal of this type of corrective control is to get that employee back on to the right track.
* The advantage of this is to catch the issues earlier and to correct them right away.
* The disadvantage is that if the employee gets 3 in fractions then he or she will be subject to termination.

1. **SilverCorp could monitor all internal communications as Technical control.**

* The goal of monitoring all communications is type of detective control.
* The advantage of this will help because of 24 hour monitoring or ill communication.
* The disadvantage of this type of solution is that the job would feel as though the employees are always being watched and scrutinized.It would result in an unhappy and unhealthy work environment.