Background:
Companies must follow data protection laws when they deal with sensitive information, and a strict code of confidentiality is a must when processing criminal record checks. If you don't protect and secure confidential information, you could lose revenue or clients, and that information could also be used unlawfully, like in fraud, if you do not even protect it. In the following content, how the workers handled well the privileged information will be discuss.

1.) Secure and lock paper documents:

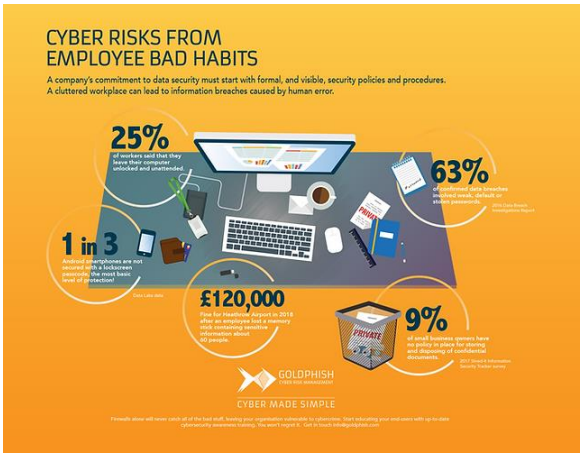
Many companies are primarily concerned with securing private information online, ignoring paper copies. Hard copies of private information are often left in plain sight on employees tables, shelves, and furniture, where there are few, if any, physical controls. Designate well-organized, locked areas for private data and instruct employees on how to use such areas. Make sure the right policies and processes are in place to support these expectations.
Example in real life: (Coca-Cola)
In April of 2021, a man named Dr. Xiaorong You, who had formerly worked for Coca-Cola, was found guilty of stealing trade secrets relating to bisphenol A. (BPA). She was charged of participating in a conspiracy, committing fraud through wire, and engaging in economic espionage. Dr. You used her phone to take pictures of top-secret papers in order to circumvent the safety precautions taken by Coca-Cola. According to the report in Chemical & Engineering News, a Chinese scientist stole information from Coca-Cola and seven other chemical businesses totaling an astounding $120 million. The information was stolen from Coca-Cola. Dr. You had every intention of selling the sensitive information to a Chinese plastic manufacture firm that had obtained government funding.

2.) Use only authorized software products to store and handle sensitive data:
In your company's rules, you should specify how and where sensitive data is kept and handled. Throughout history, a number of businesses have been publicized in the press when an employee has misplaced secret information that was kept on a USB drive or the hard disk of a laptop. The confidential information should have never been stored outside of the internal company systems, but there were no rules in place to make sure the data was handled properly.

Example in real life: (General Electric Aviation)

Example of industrial espionage is provided by the trial and subsequent conviction of Xu, which took place in November of 2021. This official of the Chinese intelligence service orchestrated an effort to get access to the exclusive aviation fan technology developed by General Electric Aviation.
When Xu was the dean of the Department of Aeronautics and Astronautics at the Nanjing University of Aeronautics and Astronautics four years ago, he asked a worker from GE Aviation to deliver a presentation there. During the course of the presentation, the host "fixed" a technical issue by placing malware on the hard drive, cloning the hard drive, or using a flash drive. After this was uncovered, the employee of GE Aviation was able to convince Xu to leave China, and the intelligence officer was placed under custody.

3.) Establish a desk and screen cleaning policy:
A clean desk policy is a good practice that may help maintain confidentiality. This will assist in reinforcing some of the key points that were mentioned earlier. At the end of the day, you want your workers to maintain as little secret information as possible on their desks and the desktops of their workstations.
The clean desk policy will provide direction on :
a.) The appropriate use of safe storage facilities as well as shredding methods for private data.
b.) What kind of data may be recorded and/or saved on portable storage devices.



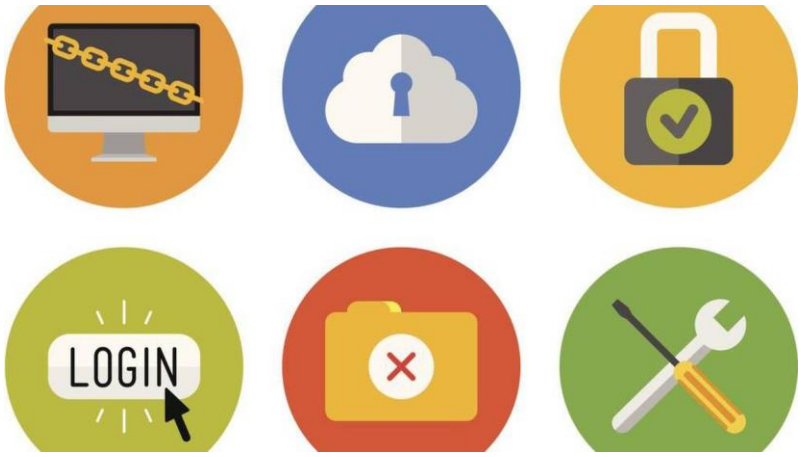
It's possible that the clean screen policy will include criteria like these:
a.) Putting a privacy filter on the monitors used by staff members.
b.) Providing users with instructions to lock their workstation desktops Users may also be technically required to lock their screens before leaving their workstations, and workstation desktops can be programmed to lock themselves after a certain amount of time if no one uses them.
Access to private information must be limited to secure devices.
a.) This rule will assist guarantee that workers do not store sensitive information on hard drives, portable media, personal devices, or any other kind of storage media that is prohibited by your company.

4.) Shred paper files when they are no longer required:
In order to make the disposal of secret information that is no longer required simple and risk-free, your company should install shredders in all of its office spaces. To be honest, Employees may resort to using the recycling container or a box on their workstations if there are no nearby shredders.

5.) Delete sensitive data from employee-owned devices and removable media upon end of employment.

Protecting sensitive information while it is "in flight" as you go about your day-to-day business is crucial; but, it is just as important to ensure that you can properly cleanse it after it has left the confines of your company and into the public sphere. When an employee leaves or is dismissed, you may protect sensitive information by remotely wiping their personal device using a Mobile Device Management (MDM) solution. An employee is obligated to maintain the highest level of trust and confidentiality with regard to any and all private information both during and after their time working for the company. If it is necessary for the employee to store, access, reveal or use sensitive information in the course of their work for the firm, then they should only do so in accordance with the company's policies. When accessing, using, or disclosing sensitive information, an employee has a responsibility to comply with all relevant state and federal laws as well as the company's own regulations. Former workers represent a potential threat to the company. It would not be difficult for a dissatisfied worker who is searching for a means to strike back at the firm or a trusted insider who is leaving for a rival to take important data belonging to an organization with them when they leave. Industrial espionage is a practice that often takes place in the last few weeks of employment, or even after an individual has been let go from their position. This often occurs when the credentials of a dismissed employee stay active, giving the former employee unrestricted access to the sensitive data held by the business without attracting anyone's attention.
In order to safeguard your organization from the possibility of former employees engaging in acts of industrial espionage, you will need to devise and carry out an appropriate method for terminating employees.

6.) Prohibit the sharing of private information with anybody outside the organization or anyone inside the organization who lacks the necessary privileges.



In the process of developing and beginning to implement the required policies and processes to preserve the confidentiality of your sensitive information, you will also need to determine who should be permitted to have access to that information. It is not necessary for an employee to have "wide open" access to all of the company's information just because they have a network account and permission to browse the general

network shares. It is recommended that employee access be set up according to the concept of least privilege. This means that employees should only have access to the information that is necessary for them to do their duties.
Example in real life: An internal document that was obtained by Motherboard revealed that Google terminated the employment of about 80 workers between 2018 and 2020 for improperly utilizing user data and spying on consumers. Some individuals even disclosed personally identifiable information to other parties. 36 of these individuals were terminated in the year 2020 as a direct result of security concerns.
Even if there is no concrete evidence to suggest that Google was a victim of industrial espionage, the possibility was always there: Mishandling of data was involved in 86% of the security-related charges levelled against workers. This included sending private material to other parties outside the company. Similar data dumps may do significant harm to a company's reputation, regardless of whether or not the incidents in question entail corporate espionage.

Conclusion:
The need of maintaining privacy and discretion is quite high in almost all professions, enterprises, and vocations. It is essential for businesses or employees to be able to manage personal details, data, and other private information in an ethical manner if they want to continue operations, maintain the confidence of the general public, and comply with certain laws and regulations. Even while the specifics of what constitutes secrecy could evolve over time, the principles behind it have not changed.

References

Protecting & Handling Confidential Information | Schwegman Lundberg & Woessner. (2019, August 29). In *Protecting & Handling Confidential Information | Schwegman Lundberg & Woessner*. https://www.slwip.com/resources/protecting-handling-confidential-information/

Johnson, B. (2022, December 7). Confidentiality Policy Best Practices | StrongDM. In *Confidentiality Policy Best Practices | StrongDM*. https://discover.strongdm.com/blog/confidentiality-policy-best-practices

https://www.sec.gov/Archives/edgar/data/1005731/000119312509217321/dex1401.htm. (n.d.). https://www.sec.gov/Archives/edgar/data/1005731/000119312509217321/dex1401.htm

4 Ways Privileged Access Management Secures Remote Workers. (2020, May 12). In *4 Ways Privileged Access Management Secures Remote Workers*. https://www.cyberark.com/resources/blog/4-ways-privileged-access-management-secures-remote-workers

How to Detect and Prevent Industrial Espionage. (2022, June 1). In *How to Detect and Prevent Industrial Espionage [with Examples] | Ekran System*. https://www.ekransystem.com/en/blog/prevent-industrial-espionage

https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2017-18/november-december/attorney-client-privilege-inhouse-counsel/. (n.d.). https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2017-18/november-december/attorney-client-privilege-inhouse-counsel/

J. (2018, May 1). Confidentiality in Business - Why Is It Important? | Care Check. In *Care Check*. https://www.carecheck.co.uk/confidentiality-why-is-it-important/

Protecting & Handling Confidential Information | Schwegman Lundberg & Woessner. (2019, August 29). In *Protecting & Handling Confidential Information | Schwegman Lundberg & Woessner*. https://www.slwip.com/resources/protecting-handling-confidential-information/