**Data Loss Prevention Policy for Laptop Computers**

**Overview:**

Data Loss Prevention Policy (DLP) explains **company’s** strategy on how to prevent data from being accessed by unauthorized users. This helps ensure not only the security of the organization, but also the security of clients that are partnering with the companyat any point in time.

At **company**, in order to make sure all data is secured and protected across the organization, we require all employees implement the following practices on their company devices and when handling other company technologies.

**Account Protection:**

DLP starts from the protection of employee accounts as many of these accounts under the employee may contain sensitive data to the company and our clients.

The following steps should be taken to ensure that all company accounts are secured.

1. Implement secure passwords on all accounts.
   1. Password Guidelines: Password is at least 8 characters long, containing letters (upper and lowercase), numbers, as well as special characters such as (but not limited to) !@#$%^&\*() .
2. Implement two-factor authentication whenever possible.
3. Always lock devices when stepping away from the workspace.
4. Sign out of accounts after each use whether on your personal work computer or another device.

**Data Protection:**

To ensure all data on devices are secured, all employees are asked to practice the following when storing data on work laptops.

1. Encrypt hard disk on laptops.
   1. If data is extremely sensitive make sure to protect the document with a password as well.
2. Use an encrypted service when sending company data
3. Employees are asked to delete data that is not being used off of laptops.
   1. Make sure that data that is deleted is not recoverable (Ex. empty recycling bin on laptop).

**Other Measures:**

In addition to the practices mentioned above, the following steps must also be implemented to ensure the extra layer of protection.

1. All data on devices must be backed up by the employee before clocking out for the day.
2. Visit and use only authorized websites through company devices.
3. Employees are asked to limit data transmission through USB drives or other peripherals.
   1. Under situations where sensitive data needs to be transmitted, use the company’s cloud to share data with coworkers.
4. Do not download data onto computers unless it is work related material that has been verified.
5. Implement laptop protection software (should already be installed on computer).
   1. This ensures that in the event that company laptops are compensated, employees are able to delete all data from the device remotely.

In the event that data is breached, notify the supervisor and IT department immediately for additional procedures. Following, make sure to remotely delete all data from the device using the laptop protection software.

If there are any questions or concerns in relation to the practices in relation to Data Loss Prevention, please contact the IT department at any point in time.

**Sources:**

<https://digitalguardian.com/blog/establishing-data-loss-prevention-policy-within-your-organization>

<https://aceits.net/employee-monitoring-as-a-data-loss-prevention-dlp-strategy/>