Cognitive Automation Labs

Bring You Own Device Policy

Table of Contents

PURPOSE

The purpose of this BYOD (Bring Your Own Device) policy is to outline the guidelines and expectations for employees who choose to use their personal devices for work-related purposes within Cognitive Automation Labs. This policy aims to ensure the security, confidentiality, and integrity of company data while respecting the rights and privacy of employees.

SCOPE

This policy applies to all employees, contractors, consultants, and any other personnel who use personal devices to access company resources, networks, systems, or data. It encompasses all types of personal devices, including but not limited to smartphones, tablets, laptops, and wearable devices.

ELIGIBILITY AND PARTICIPATION

3.1. All employees who wish to use their personal devices for work-related purposes must voluntarily participate in the BYOD program.
3.2. Employees must adhere to this policy and any additional rules or procedures set forth by the CA Labs IT department.
3.3. The company reserves the right to deny or revoke participation in the BYOD program if deemed necessary.

DEVICE SECURITY AND COMPLIANCE

4.1. Employees are responsible for maintaining the security of their personal devices, including implementing strong passwords, using biometric authentication where available, and regularly updating the operating systems and applications to the latest versions to ensure effective security patching is applied.
4.2. Devices must be protected by approved security measures, such as antivirus software and device encryption.
4.3. Jailbroken, rooted, or otherwise compromised devices are strictly prohibited from accessing company resources.
4.4. Lost or stolen devices must be reported immediately to the IT department and the appropriate security measures, such as remote wiping or device tracking, will be implemented, if available.
4.5. The company reserves the right to remotely manage and monitor personal devices to enforce security policies, perform updates, or protect company data.

DATA AND INFORMATION SECURITY

5.1. Employees must exercise due diligence in protecting company data and information accessed or stored on personal devices.
5.2. All work-related data must be stored in approved company applications, cloud services, or network drives. Personal cloud storage solutions are prohibited for company data.
5.3. Employees must not share company data with unauthorized individuals or use it for personal purposes.
5.4. Company data stored on personal devices should be encrypted and regularly backed up.
5.5. In the event of termination, resignation, or any change in employment status, the IT department may remotely wipe all company data from the personal device.

Cognitive Automation Labs

ACCEPTABLE USE

6.1. Personal devices should be used responsibly and in compliance with all applicable laws, regulations, and company policies.
6.2. Employees must not use personal devices to access or create any illegal, offensive, or inappropriate content.
6.3. Personal devices should not interfere with the work environment, productivity, or confidentiality of others.
6.4. The company reserves the right to restrict or block certain websites, applications, or content that pose security risks or violate company policies.

SUPPORT AND MAINTENANCE

7.1. Employees are responsible for the support and maintenance of their personal devices. The company will not be liable for any device malfunction, damage, or loss.
7.2. The IT department will provide limited support for connectivity and access to company resources. However, troubleshooting personal device issues may be limited.

POLICY VIOLATIONS

8.1. Any violation of this BYOD policy may result in disciplinary action, up to and including termination of employment or legal action, depending on the severity and impact of the violation.
8.2. Employees must report any suspected breaches or security incidents involving personal devices to the IT department immediately.

POLICY REVIEW

Cognitive Automation Labs may make changes to this policy from time to time.

Prepared by:	Joanne Parsons – Head of Business Administration
Approved by:	Jonathan Parsons – Co-Founder & CEO
Last Modified:	14/12/2021