BRING YOUR OWN DEVICE POLICY (BYOD)

NextGen CGI, LLC

Document Owner: NextGen CGI, LLC
Effective Date: January 1, 2021
Updated:

NextGen CGI, LLC BYOD Policy							
Effective Date:				**Document Owner:**			
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0	01/01/2021	Policy	S. Hall	S. Hall	01/01/2021	S. Hall	01/01/2021

BYOD Policy
Version 1.0
January 1, 2021

1. Purpose

The policy purpose is to outline standards, procedures, and restrictions for users connecting a personal device to NextGen CGI's organization network for business purposes. The following devices and media apply to this policy:

- Smartphones
- Other mobile/cellular phones
- Portable media devices
- Laptop/tablet computers, including home desktops
- Any personally owned device capable of storing organizational data and connecting to a network

Any hardware and related software that is not owned or supplied by the organization but could be used to access organizational resources applies. Including devices that employees have acquired for personal use but also wish to use in the business environment.

2. Goal

The policy goal is to protect the integrity of confidential business data located within NextGen CGI's technological infrastructure. This policy aims to prevent data from being stored without ample security on a device or carried over an insecure network where unauthorized access may occur. A breach could result in loss of information, damage to critical applications, and damage to the company's image. Users using a personal device connected to NextGen CGI's network, and able of backing up, storing, or accessing data of any type, must follow company defined procedures.

3. BYOD Policy

NextGen CGI allows employees to purchase and use devices, noted in section 1, of their choosing at work for their convenience. NextGen CGI reserves the right to retract this privilege upon users not abiding by the policies and procedures outlined in this document.

This policy protects the security and integrity of NextGen CGI's data and technology infrastructure. Exceptions to the policy may occur due to changes in devices and platforms.

NextGen CGI terms and conditions in this policy must be agreed upon by employees in order to connect their devices to the company network.

4. Stipend Guidelines

NextGen CGI will offer a stipend of $1,800 to eligible employees every 2 years to purchase a device that can be used for both business and personal use. The stipend should be used to cover the following:

- Cost of device/operating system
- Required business productivity applications
- Anti-virus software
- Service contract

Approval of devices by IT is required before purchase. Consult with IT about minimum requirements of the device being purchased. The employee may exceed the stipend amount at their own expense.

A mobile phone with work email set up is eligible to receive a discount credit from NextGen CGI to apply toward a monthly plan from any carrier.

Refer to section 10 for stipend guidelines upon termination, retirement or resignation.

5. Acceptable Use

It is the employee's responsibility if using a personal device to access business resources to ensure all security protocols normally used in management of data are applied. It is imperative that any mobile device used to conduct NextGen CGI business be utilized appropriately, responsibly, and ethically. Failure to comply will result in immediate suspension of that user's account.

NextGen CGI defines acceptable business use as activities that directly or indirectly support the business. Devices may not be used at any time to:

- Store or transmit illicit materials
- Store or transmit proprietary information belonging to another company
- Harass others
- Engage in outside business activities

6. Access Control

Prior to use of a personal device on the organization network or related infrastructure, all devices must be approved by the IT department. NextGen CGI will maintain a list of approved devices with appropriate control requirements at Access Control. Devices that do not appear on this list may not be connected to organization infrastructure. If your preferred device does not appear on the approved list, contact the IT help desk.

Devices attempting to connect to the company network through the internet will be inspected using technology centrally managed by NextGen CGI's IT department. Devices not previously approved by IT, are not in compliance with IT's security policies, or represent any threat to the company network or data will not be allowed to connect. Devices may only access the organization network and data through the internet using a VPN or other secure network. The VPN portal web address will be provided to users as required. Smart mobile devices such as smartphones and tablets will access the company network and data using mobile VPN software installed on the device by IT.

End users wishing to connect devices to non-organizational network infrastructure to gain access to company data must employ, for their devices and related infrastructure, security measures communicated by the IT department. Company data is not to be stored on or accessed from any hardware that fails to meet NextGen CGI's established company IT security standards.

IT reserves the right to refuse the ability to connect personal devices to the network and infrastructure. IT will engage in such action if such equipment is being used in a way that puts the company's systems, data, users, and clients at risk. IT reserves the right to update the approved device list at any time.

Management reserves the right to review or retain personal and company related data on personal devices or to release the data to government agencies or third parties during an investigation. Management may review the activity and analyze use patterns and may choose to publicize this data to ensure NextGen CGI's resources are being used according to this policy. No employee may knowingly disable any network software or system identified as a monitoring tool.

7. Support for Devices

Employees who elect into the BYOD program are not eligible for support for device-specific hardware or software from NextGen CGI's IT department. If the device requires maintenance, the employee is responsible for taking the device to the business-approved third-party support provider as designated by the provider. IT will provide the employee with a business owned device [laptop, desktop, thin client] for the duration of the maintenance period.

NextGen CGI's IT department will prioritize support calls to determine if the issue is software or hardware related. If the issue is hardware related, the employee will be forwarded to the third-party support provider for maintenance. If the issue is software related or related to virtual or web-based applications, the IT department will perform maintenance.

Employees, contractors, and temporary staff will make no modifications to the hardware or software that change the nature of the device in a significant way without approval of NextGen CGI's IT department.

8. Security

Employees using personally owned devices and related software for network and data access will use secure data management procedures. All devices that are able to store data must be protected by a strong password and data stored on the device must be encrypted. See NextGen CGI's password and encryption policy at [file location] for additional requirements. Employees agree never to disclose their passwords to anyone or store passwords on personally owned devices.

Users of personally owned devices must use reasonable physical security measures. End users are expected to secure all devices whether or not they are in use or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain company data.

Any non-business computers used to synchronize with these devices will have installed updated anti-virus and anti-malware software deemed necessary by NextGen CGI's IT department. See [file location] for anti-virus requirements and recommendations.

Passwords and other confidential data defined by NextGen CGI's IT department are not to be stored unencrypted on mobile devices.

Any device that is being used to store NextGen CGI data must adhere to the authentication requirements of NextGen CGI's IT department. Hardware security configurations must also be pre-approved by NextGen CGI's IT department before any company data carrying device can be connected to the organizational network.

IT will manage security policies, network, application, and data access centrally using technology solutions seen suitable. Any attempt to violate or bypass security implementation will be deemed an intrusion attempt and will be dealt with in accordance with NextGen CGI's overarching security policy.

IT reserves the right, through policy enforcement and any other resources necessary, to limit the ability of end users transferring data to and from specific resources on company network.

Employees, contractors, and temporary staff will follow all company sanctioned data removal procedures to erase company specific data from devices once its use is no longer required. See [file location] for detailed data wipe procedures for eligible devices.

In the event of a lost or stolen device, it is mandatory for the user to report the incident to IT immediately. The device will be remotely wiped of all data and locked to prevent unauthorized access. If device is recovered, it can be submitted to IT for re-provisioning. Appropriate steps will be taken to ensure that company data on or accessible from the device is secured - including remote wiping of the device where appropriate. The remote wipe will destroy all data on the device, whether it is related to company or personal use.

9. Termination of Employment

In the event of termination, retirement or resignation, the employee must reimburse a prorated amount of the stipend. The prorated amount is based on the number of weeks/months remaining in the 2 year period. The amount will be gathered from final paycheck where possible and any outstanding amount will be charged to the employee to be collected within 30 days of the last day worked.

Upon termination, retirement or resignation, the user must take their device to NextGen CGI's IT department to be inspected. Following inspection, the user's access will be terminated to company infrastructure.

10. Failure to Comply with Policy

Failure to comply with the BYOD Policy may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, possible termination of employment, as well as possible criminal charges.

11. Roles and Responsibilities

Role	Responsibility

Chief Information Officer	• Overall responsibility for the confidentiality, integrity and availability of company data
IT Staff	• Responsible for updating accepted device list • Perform Helpdesk tasks to maintain company devices and infrastructure
Users/Employees	• Responsible for purchase of device • Responsible for complying with all policy standards

12. Related Standards, Policies, and Processes

- Password and Encryption Policy
- Security Policy
- Incident Response Policy
- Disaster Recovery Plan
- Vendor Management Policy
- Acceptable Use Policy

13. Definitions and Terms

The following definitions are not all-inclusive and should be updated as new information is made available:

Term	Definition
None	None