BGCA Bring Your Own Mobile Device Policy

Introduction

This policy covers the use and security of personally-owned mobile devices while storing or accessing company information. This policy is intended to protect the security and integrity of Boys & Girls Clubs of America's data and technology infrastructure.

Purpose

Boys & Girls Clubs of America (BGCA) permits its employees to use personal smartphones and tablets of their choosing at work and for work-related activities. Personal mobile devices present an ever-increasing threat to corporate networks as their vulnerabilities do not have the same protection available to company-issued personal computers. BGCA reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below for smartphones, tablets and other mobile electronic devices that can access and store BGCA information.

Scope

Mobile devices (e.g., cell phones, tablets, and smart watches) that access or store company information.

Exceptions

None

Policy and Acceptable Use

BGCA defines acceptable business use as activities that directly or indirectly support the business of BGCA. The following are practices that employees should be aware of at all times:

- All personally-owned mobile devices which access BGCA systems and data (e.g., email and files) must have the following security features enabled:
    - Power-on passwords
    - User account passwords that meet or exceed existing domain password requirements
    - Software updates
    - BGCA provided (or approved) endpoint security

- Mobile devices belonging to employees that are for personal use only are not allowed to connect to the corporate network.

While conducting BGCA business, the employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's HR Employee Handbook, IT Acceptable Use policy, Endpoint IT Security Policy, IT Wireless Networks Policy, IT Passwords Policy

- As long as endpoint protection and mobile device management requirements are met, employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, and documents.

- It is the responsibility of the user to ensure that backups of personal data are being made.

- Users must report any threat or unauthorized access or breach of any mobile device that has access to BGCA assets including email or any proprietary information.

Devices and Support

- BGCA does not endorse or have preferences on the types of mobile devices an employee uses for business as long as those devices can be in full compliance with the requirements noted in the Policy and Acceptable Use section of this document.

- Employees should contact the device manufacturer or their carrier for operating system, hardware, or connectivity-related issues.

- BGCA reserves the right to block access to its networks and systems to any device that does not adhere to Policies and Acceptable Use rules.

- The employee is personally liable for all costs associated with his or her device

Roles and Responsibilities

It is the responsibility of the individual device user to ensure that this policy is adhered to. It is the role of management to ensure that this policy is enforced.

The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

How Compliance will be Measured

Actions for Policy Violations

Management reserves the right to perform random inspections at any time to ensure the device is compliant with BGCA policy.

- First violation: The user will receive an automated system alert or, when applicable, a notice from IT Security specifying the incident and actions needed by the user to correct the issue. Refer to Appendix in this document as a reference for repeated notifications and user privacy.

- A Second violation:
    - A warning and documented violation sent to user and direct supervisor
    - At this time, the user may be banned from use of personal devices
    - If the user is permitted to use their device, the user will be required to complete additional security training
        - Failure to complete this training within 72 after the written warning will result in a system lockout for the user until their training is compete and verified on the Knowbe4 system managed by BGCA IT Security.

- A Third violation – warning and documented violation sent to user, direct supervisor, and SLT executive. IT leadership will need to meet with direct supervisor and, if necessary, SLT member and HR to discuss further recourse included a ban on this user being permitted to access BGCA networks or possess BGCA information on their devices.

Review and Evaluation

Boys & Girls Clubs of America shall review, evaluate, and document the outcome of each of the following at least once a year:

- Effectiveness of this policy
- Maintenance costs of this policy to the business
- Impact of policy controls to the business
- Impact of policy on technical infrastructure requirements

In addition, this policy shall be revised as needed based on, but not limited to, any of the following:

- Significant security incidents that have occurred
- New vulnerabilities discovered during ongoing security assessments or annual audits
- Changes to the organizational structure
- Changes to the information technology infrastructure

Related Documents

HR Employee Handbook
Acceptable Usage Policy
Endpoint Security Policy
Wireless Networks Policy
Passwords Policy

Revisions

Draft version 1 created by Kevin Beaver on January 9, 2018
Version 2.0 created by Mat Mathews 03 September 2018
Version 2.1 updated by Mat Mathews with review and edits by Sybil Hadley 02 May 2019
Version 2.2 updated by Mat Mathews to implement changes by Stan Kubis 04 June 2019
Version 2.2.1 updated by Mat Mathews to implement changes discussed at 10 June 2019 Mobile Device Committee Meeting

Appendix 1: Privacy and BGCA ITSecNet Governance related to Mobile Device Security Alerts for Malicious Applications

The following outlines how alerts are managed from a privacy perspective.

Step 1: The Mobile Device Security Application alerts the user and BGCA IT Security with an auto generated email notification that a specific app is malicious (i.e., the application is putting the user's entire phone and subsequently BGCA information at risk).

Step 2: The user is notified by BGCA IT Security and a request will be made to the user asking them to remove the malicious app. No information about this incident will be disclosed outside of IT Security. All incidents will be addressed on case by case and all efforts will be made to achieve a resolution that is in the best interest of both the user's and BGCA's security and privacy.

Step 3: If the user ignores the first request to address the alert. They will be sent a second request from BGCA IT Security, with a warning that access to BGCA email and other BGCA Intranet will no longer be available from their phone if they do not comply in 5-days.

Step 3: The user ignores the second request. After 5-days, a notice of access cut-off from the mobile device will be sent to the user. BGCA IT Security will work with IT Operations to remove and block the user's access to BGCA email and BGCA sites from their phone.

Step 4: The user must demonstrate to BGCA IT Security that the malicious app has been removed through validations from the Mobile Device Security Application.

The following measures that will be taken to ensure privacy.

Measure 1: If the user's manager approaches BGCA IT Security as to why the user is no longer granted access to their email or BGCA Intranet via their phone, BGCA IT Security can disclose to the manager that the user had an application on their phone posed a risk to BGCA and was not removed after two warnings.

Measure 2: If the manager inquires as to the name or nature of the app. That information will not be disclosed. Such information is deemed restricted to BGCA IT Security.

Measure 3: Should a member of BGCA IT Security disclose information beyond what is described above without and order and authorization from General Counsel and HR, that individual could be removed from the team, and/or dismissed from the department, and/or have a their employment terminated.