**CYB-250**

**Policy Update**

**Candace Ralston**

**2/10/2023**

This is the updated version for the Bring Your Own Device (BYOD). This is because we have noticed that more people are bringing their own devices in to use. When the policy was originally written not many people if at all were bringing their own devices. So, it was decided that we needed to update the BYOD so that we can make sure it covers everything that could and may happen. Also, with this new policy it will not allow the employees to deviate from it or make assumptions about it. It can cause a big problem if the employees think they can deviate from the policy. Some of the sections of the new policy are:

|  |  |
| --- | --- |
| **Original BYOD Policy**  **Acceptable Use** | **New BYOD Policy**  **Acceptable use** |
| The organization defines acceptable use as activities that are personal in nature and do not involve any business function. | The organization defines acceptable use as able use personal devices for work and personal use. |
| The organization defines acceptable personal use during business hours as reasonable and limited personal communication or recreation, such as reading or game playing. Acceptable personal use during business hours should only occur during break or lunch times. | The organization defines acceptable use as able to use personal devices only for work during business hours. For recreational use such as reading or gaming only for break or lunch times. |
| Employees are blocked from accessing certain websites during work hours and while connected to the network at the discretion of the organization. | Employees will be blocked from accessing certain websites during work hours and while connected to the network. This includes during break and lunch times. |
| Devices’ camera and/or video capabilities are not disabled while connected to the network. | Personal devices’ camera and video capabilities will not be used during business hours. |
| Devices may not be used at any time to:   * Store or transmit any information belonging to the organization * Conduct regular business for the organization during normal business hours * Engage in activities in performance of duties for another organization | Devices may NOT be used at any time to:   * Store or transmit any information belonging to the organization * Conduct regular business for the organization during normal business hours * Engage in activities in performance of duties for another organization |
| Personal devices may be used to access organizational email, calendars, and contacts. | Personal devices may be used to access organizational email, calendars, and contacts only during normal business hours. |

|  |  |
| --- | --- |
| **Original BYOD Policy**  **Devices and Support** | **New BYOD Policy**  **Devices and Support** |
| Smart devices and tablets such as iPhone, Android, iPad, or any other smart devices are permissible for use. | Only smart devices and tablets that are iPhones, Android, iPad, Samsung tablet, and laptop are permissible for use. |
| Connectivity issues may be supported by IT on a limited basis. | Any connectivity issues may be taken to IT on a limited basis. |
| Devices must be presented to IT before they can access the network. | Devices will be presented to IT before they can use the network. |

|  |  |
| --- | --- |
| **Original BYOD Policy**  **Security** | **New BYOD Policy**  **Security** |
| In order to prevent unauthorized access, devices must be password protected using the features of the device at all times. | To prevent unauthorized access, all devices must be password protected using the features of the devices at all times. |
| A strong password is required to access the company network. Passwords must be at least six characters and a combination of upper- and lowercase letters, numbers, and symbols. | A strong password is required to access the company network. Passwords must be at least eight characters long and have a combination of upper-and-lowercase letters (a, b, c, A, B, C), numbers (1, 2, 3), and symbols (!, @, #, $, %). |
| The device will have security software, owned by the organization, installed for use in multifactor authentication. | The device must have the security software from the organization, installed for the use in the multifactor authentication. |
| After eight failed login attempts, the device’s access to the network will be suspended. IT must be contacted to have access to the network reinstated. | After four failed login attempts, the device’s access to the network will be suspended. IT must then be contacted to get the access to the network reinstated. |
| Smart devices and tablets that are not presented to IT for clearance will not be allowed to connect to the network: no exceptions. | All smart devices and tablets that are not presented to IT for clearance will not be allowed to connect to the network: NO EXCEPTIONS. |
| The employee’s device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus, or similar threat to the security of the organization’s data and technology infrastructure. | The employee’s device will be remotely wiped if:   * The device is lost * The employee terminates his or her employment * IT detects a data or policy breach, a virus, or similar threat to the security of the organization’s data and technology infrastructure |

|  |  |
| --- | --- |
| **Original BYOD Policy**  **Risks/Liabilities/Disclaimers** | **New BYOD Policy**  **Risks/Liabilities/Disclaimers** |
| While IT will take every precaution to prevent the employee’s personal data from being lost in the event it must remote wipe a device, it is the employee’s responsibility to take additional precautions, such as backing up email, contacts, etc. | It will be the responsibility of the owner of the device to back up emails, contacts, etc. in the event of the device needing to be remotely wiped because of it being lost or stolen. |
| The company reserves the right to disconnect devices or disable services without notification. | The company has the right to disconnect devices or disable services WITHOUT NOTIFICATION. |
| The employee is expected to use their devices in an ethical manner at all times and adhere to the organization’s acceptable use policy as outlined above. | The owner of the device is expected to use the device in an ethical manner at all times when using it for work and will adhere to the organization’s acceptable use policy as outlined above. |
| The employee is personally liable for all costs associated with their device. | The owner of the device is personally liable for ALL costs associated with their device, like buying more storage: NO EXCEPTIONS. |
| The employee assumes full liability for risks including, but not limited to, complete loss of 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. | The owner of the device is liable for all the risks of the device including, but not limited to, complete loss of personal data due to a system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable: NO EXCEPTIONS. |
| The organization reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy. | The organization has the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy. |

There would be a lot of impacts that this policy would have on this organizational culture. For one thing if I knew that I was being monitored on my personal device at work I would watch what I am looking at on my device. Also, I would need to watch what people send me with my email, something that was send could be misconstrued and I could get into trouble. You would of course always have to make sure that you watch what you look at and what you are sending when you are at work not just on your own device.

There are a lot of things to think about when updating the BYOD. Another part of the policy that could be considered, especially with more people bringing their own devices to work is training. People really need to understand what it means to have this policy. The best way to do that would be to have a meeting explaining what the policy is about. The employees need to know what they are getting into when they start bringing their own devices. If they don’t understand the policy, they may choose to ignore it and do their own thing. Understanding any policy would be the first thing to do in order to make sure that people understand that it is there.