WIZ ACCEPTABLE USE & MONITORING POLICY

Content

1. Purpose

This purpose of this Policy is to explain:

- what you can and can't do with your **Wiz Hardware** (this means your Wiz laptop/desktop, desk phone/ smartphone and any other hardware provided to you by Wiz or used to access Wiz's IT Systems (which could include your personal smartphone));
- how you should use **Wiz's IT systems** (which include our computer network, storage, hardware, software, phones, Internet and other IT systems), both when working from the office and remotely;
- when Wiz may need to monitor or access your usage and how we will do it; and
- your obligations to keep a clear desk and clear screen.

We may make changes to this Policy from time to time. If there are any changes to this Policy we'll let you know.

If you have any questions about this Policy or you're not sure how you should act in a specific situation related to this Policy please contact legal@wiz.io and/or security@wiz.io.

2. Application

This Policy applies to all Wiz employees, officers and contractors or anyone else who has Wiz Hardware and/or access to Wiz IT Systems (together "**Personnel**").

For more info about what personal information we process about you, please read Wiz's Employee and Contractor Privacy Notice which

is available in Wiz's internal HR information system.

3. Responsibility

All Personnel are responsible for knowing and complying with all aspects of this Policy. Breach of this Policy may lead to disciplinary action and, in serious cases, may be treated as gross misconduct leading to dismissal.

If you become aware or suspect any violation of this Policy, you must report it to your manager, HR, or Wiz's Legal team.

4. Policy

What's the bottom line?

- Your use of Wiz Hardware and IT Systems is not unlimited and is subject to conditions and restrictions. **We strongly recommend that you do not use your Wiz IT Systems or Hardware for personal use.**
- You're responsible for using Wiz Hardware and IT Systems safely and protecting it appropriately.
- We perform routine and (in certain cases only) specific monitoring of your usage for security, troubleshooting and maintenance purposes in accordance with local laws and requirements in your jurisdiction. We don't actively review your browsing history or personal files (unless we have legitimate reasons to in accordance with local laws) - everything we monitor is in order to keep Wiz information and systems safe.
- You are responsible for complying with this policy and ensuring that you keep a clean desk and clear screen.

5. Use of Wiz Hardware

Your Wiz Hardware contains important and confidential information, so we expect you to apply common sense and protect it appropriately.

Specifically, we expect you:

- Not to leave your laptop or phone unattended.
- To lock your workstation when unattended.
- Not to upload confidential company data to unauthorized platforms.
- To use a strong password (using a combination of uppercase and lowercase letters and numbers) and to change it regularly.
- Not to share your Wiz password(s) or access codes with anyone else.
- Not to attempt to discover or use Wiz password(s) or access codes of any other Wiz Personnel.

6. Use of Wiz IT Systems

As a user of Wiz's IT Systems, you have access to valuable resources and sensitive data. Consequently, you are expected to behave responsibly, ethically, lawfully and in accordance with the below instructions:

- **Personal use**: Wiz IT Systems and Hardware are made available to you for work related purposes. **Whilst it is possible for you to use your Wiz IT Systems or Hardware for reasonable personal use, we strongly recommend that you do not do so, and any such use must be in line with this Policy and must not harm your work or Wiz's business.** If you save personal files (such as personal photos, personal emails, documents, etc.) on Wiz IT Systems please note that:
    - You generally do not have a right to privacy when using Wiz Hardware and IT Systems.
    - Your personal files may be copied as part of routine back-up procedures so, even if you delete them from your laptop, a backup copy may still be stored on other Wiz IT Systems.
    - Wiz staff may have incidental access to your personal files during maintenance and troubleshooting activities.

    - We may, from time to time and **WITHOUT** any prior notification, permanently remove any personal files stored on Wiz IT Systems. So we recommend that you always keep a back-up copy of your personal files somewhere else.
    - We may access your personal files as part of specific or general monitoring (see further details in the "Monitoring of Wiz IT Systems" section below.
    - If you leave Wiz, your personal files may reside on Wiz's systems.
- **Access and permissions**: Your access to Wiz IT Systems is **not unlimited.** Access to certain sensitive or confidential information is intended only for those who have a **need to access it**. You shouldn't attempt to access any Wiz IT System or information which you are not authorized to and any attempt to do so or to circumvent, modify or disable Wiz IT security measures (such as access controls, firewalls, anti-virus software or intrusion protection systems), is a severe violation of this Policy.
- **Emailing and communicating data or files outside of Wiz**: This is acceptable in the ordinary course and for purposes of legitimate Wiz business, subject to your discretion and judgment. However, do not email or communicate data or files that contain sensitive company or customer information to anyone outside of Wiz, unless expressly permitted in writing by your immediate manager and only as specifically instructed by them. If you're a manager and in doubt about whether to permit the transfer of sensitive information, please contact the legal team at legal@wiz.io.
- **Emailing and communicating data or files within Wiz:** You should only communicate data or files that contain sensitive information with those who have a business need to receive them.
- **Storing Company information**: You should only save, store and back-up Wiz information on Wiz IT Systems and not on any personal computer or device.
- **Old devices:** if you no longer use your Wiz laptop, phone, or other storage device, you must return it to the IT team as soon as possible.
- **Lost or stolen devices**: notify the IT team immediately via it@wiz.io if your Wiz device is lost or stolen.
- **Prohibited content**: You should not access, download, copy, store or transmit any of the following via Wiz IT Systems:
    - Copyright-infringing and other IP-infringing content (such as pirated music, software, movies, etc.)
    - Sexually oriented content or websites
    - Computer viruses, Trojan horses, email bombs, malware, or adware
    - Unlawful content (e.g., violence, hate-speech)
    - Content otherwise prohibited by Wiz corporate policies
    - Inform the IT team immediately via it@wiz.io if you suspect that you have been sent, or have accessed a phishing email or malicious software such as viruses, Trojan horses, or email bombs.
- **Software Tools:** You may only use tools which have been approved by Wiz's procurement, security and legal and which are configured to be accessed through your Okta account. If you would like to request a new software or vendor, you should submit a request to Wiz's procurement team using this online form: https://beyondnetworkscom.sharepoint.com/sites/Procurement. Wiz's procurement process is also explained here.
- **Network and email activities:** Laptops that Wiz designates to you are configured to automatically execute virus-scanning software at frequent intervals. Do not circumvent or tamper with these virus scans. You may not (unless otherwise approved in writing in advance by the IT department):
    - Establish a private network on or through Wiz IT Systems.
    - Connect a wireless router/bridge to any Wiz IT System.
    - Engage in, or attempt to engage in, any form of email spoofing, data snooping, port scanning or security scanning on Wiz IT Systems.
    - Send unsolicited email messages, spam or "junk mail" through Wiz IT Systems.
- **Discovery/ disclosure in legal proceedings:** From time to time, Wiz may be involved in legal proceedings which require us to search for and disclose electronic information to outside parties. In such cases, materials, including your personal information and personal files that you save on Wiz IT Systems, may be processed and reviewed by Wiz or third-party service providers as part of or in anticipation of electronic discovery, and, if relevant, may be disclosed to third parties or the court.

7. Use of Wiz Email Account

- Your Wiz email account should be used for professional, work-related business purposes only.
- While you may use your personal email account (like your Gmail) on Wiz's IT Systems in accordance with the instructions

above, you **should not use your Wiz email account for any private or personal communications.** This is to reduce the exposure of your private and personal communications to monitoring measures applies to Wiz IT Systems (as further explained below).

- Wiz may monitor and access email messages sent to or from any email account at Wiz. Therefore, messages communicated through your Wiz email account are not considered or treated as private or personal.
- If you have been using your Wiz email account for private or personal use, please transfer all of your communications to your personal email address and delete them from your Wiz email account. We also ask you to inform your friends, family members and other contacts not to send personal messages to your Wiz email account.
- Wiz's email account servers may be configured to automatically attach to outgoing emails a standard footer in the format determined by Wiz's legal counsel. **Please don't remove this email footer**.

8. Use of Instant Messaging

Slack

- Wiz authorizes you to use Slack as an instant messaging service to communicate with other Wiz Personnel and customers for general business communications subject to the following restrictions:
    - You should only use Slack to the extent necessary, and only with those Wiz Personnel who have a need to know
    - You should only communicate business sensitive information via 1:1 chats or in specific closed groups, NOT in any general/public company channels
    - **Do not share any Wiz customer platform findings via Slack**

Other instant messaging services

- Other than Slack, you should not use any other instant messaging services (e.g. WhatsApp) for business communications or to share any confidential information relating to Wiz or its customers.

9. Monitoring of Wiz IT Systems

Why do we need to monitor?

We need to monitor and, sometimes, access information stored on or communicated through, Wiz's IT Systems for the following reasons:

- To protect our IT security, including to monitor, detect or block the use of files, accessories or devices that should not be stored on or connected to Wiz IT Systems.
- To prevent unauthorized transmission of information through Wiz IT Systems.
- To ensure that user conduct is in line with Wiz's policies and procedures, which can be accessed via the HR Information System.

As part of our monitoring measures, subject to local laws and requirements, information about the specific conduct may be monitored and logged including: the content of files or devices, the identity of the user and logs of the user's behavior. This information is processed in accordance with local laws and regulations. **As explained above, for this reason, we recommend that you don't store personal / private information on your Wiz computer or drives.**

How do we monitor?

We may conduct monitoring in the following ways:

- **General and continuous monitoring:** In most cases, this type of monitoring will be automated such as by using firewalls which autonomously monitor data transmission by username and destination. We may also combine manual monitoring as needed.
- **Specific monitoring:** we may conduct specific monitoring if we suspect misconduct, violation of this Policy or any other Wiz policies or ethical codes, or when we believe that there is a justifiable need.

10. Access to your devices

Maintenance of Wiz's IT Systems

Our IT team may remotely log in to your workstation or laptop, with or without seeking your consent or notifying you in advance, in order

to perform maintenance or troubleshooting activities.

Specific monitoring

If we have a justifiable reason to conduct specific monitoring and/or access your Wiz Hardware, use of the Wiz IT Systems or your Wiz Email Account (e.g. for security reasons) we will try to contact and speak with you first before taking any action where it is practical to do so. However, there may be circumstances in which we need to conduct specific monitoring without your approval. In such cases, applicable local laws will be followed and Legal and HR will be notified and involved.

Recording of calls

Wiz or its third party service providers (such as Gong) may record Zoom calls made by our customer support and/or marketing / sales teams and collect performance data or in order to monitor and improve user service and sales.

11. Clean Desk & Clear Screen

Wiz maintains a clean desk and clear screen policy. You must not leave any confidential documents or other paperwork on your desk or in your workspace and that you lock your screen whenever you are away from your desk. You are also required to remove any personal items from your desk or workspace at the end of each working day.

12. External Services

All Wiz employees are required to ensure no Wiz confidential data is shared with external services unless they have been specifically authorized by Wiz's procurement team. Such services include, but are not limited to, AI-based systems like ChatGPT, browser extensions like Grammarly, file storage and sharing servies like iCloud and/or Dropbox, note-taking services like Evernote, and social media. Employees that require the use of new external services to support their work should follow Wiz's technology procurement process to ensure the vendor can be properly reviewed, approved, and onboarded.

13. Social Media

Social media (sometimes referred to as social networking or Web 2.0 technologies) are online services and tools used for publishing, sharing and discussing information. They can include forums, blogs, wikis, social networking websites, and any other websites that allow individual users to upload and share content.

Employees are responsible for content they publish in social media and can be held personally liable for content published. Employees can also be subject to disciplinary action by the agency for publishing inappropriate or classified content. These guidelines only cover a sample of all possible content publishing scenarios, and are not a substitute for good judgment. It is important to note that these guidelines apply to all social media publishing whether personal or agency sponsored.

_____ 2023-03-21

Signature of Ryan Kazanciyan, CISO Date