WIZ ACCEPTABLE USE & MONITORING POLICY

1. Purpose and Scope

This purpose of this Policy is to describe how users can and cannot use Wiz Hardware and IT Systems, as well as how Wiz may monitor usage.

The scope of this Policy applies to all Wiz Personnel who have access to Wiz Hardware and/or IT Systems. This policy applies to the corporate controls environment.

2. Definitions

2.1 Wiz Hardware

Any physical technology provided to you by Wiz or used by you to access Wiz IT systems. This includes but is not limited to laptops,

desktops, desk phones, and smartphones (including personal devices, if used to access Wiz IT Systems).

2.2 Wiz IT Systems

Technologies and networks which provide Wiz services or which store, contain or process Wiz information. This includes but is not limited to computer network, storage, Wiz Hardware, software, phones, internet, browsers, and other IT systems.

2.3 Wiz Personnel

All Wiz employees, officers, and contractors.

Policy

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

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 cause for termination.

If you become aware or suspect any violation of this Policy, you must report it to your manager, Human Resources, or Legal.

4. Summary

- 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.
- For information about what personal information we process about you, please read Wiz's Privacy Notice for Employees, Contractors, and Workers which is available in Wiz's internal information system.

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:

- To lock your workstation when unattended, including in a Wiz office or shared space.
- To use a privacy screen if working in public spaces (e.g., coffee shop, airplane, etc.)
- Not to leave your laptop or phone unattended.
- Not to upload confidential company data to unauthorized platforms.
- 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.

Mobile Devices: For additional information specific to mobile devices, refer to the Wiz Mobile Device and Applications Management Policy.

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, we strongly recommend that you do not do so.** Any personal use of Wiz resources must be compliant with this policy and must not harm or impair your work or Wiz's business or business interests.

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. 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. We recommend that you always keep a back-up copy of your personal files on your personal hardware or IT system.
- 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.

Wiz does not restrict your use of personal mobile devices in Wiz physical offices; however, any personal devices are restricted from accessing Wiz development and production systems. Please be mindful that any use of personal mobile devices on Wiz premises may be subject to this policy insofar as you utilize Wiz IT Systems (including the internet).

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. 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.

Internet: Your use of the Internet, insofar as it is a Wiz IT System, may be restricted for security and business protection. Wiz blocks

access to malicious websites; any attempt to circumvent this control is a violation of this policy. Non-business internet sites should be used judiciously and should not negatively impact your work for Wiz, nor should it be used to transmit or store Wiz information.

Software Tools: You may only use software (including web browser extensions) which has been approved by Wiz's Procurement, Security and Legal teams 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 the process established in the Purchasing Policy.

Personal Email Tools: Personal email applications should not be used on Wiz machines as they are not Wiz-approved software. If you need to access personal emails on your Wiz laptop, please do so from your web browser.

Storing Wiz Information: You should save, store, and back up Wiz information only when necessary and only on approved IT Systems and not on any personal computer or device.

Posting Wiz information: all content must be reviewed for non-public, confidential, or proprietary data before the content is physically or electronically posted in a publicly accessible location.

Old devices: if you no longer use your Wiz laptop, phone, or other storage device, you must return it to the IT team.

Lost or stolen devices: A lost or stolen Wiz device represents a significant risk and should be addressed in a timely manner. However, your welfare and physical safety are most important. If you are separated from your device(s) in an incident involving a threat to your personal safety, don't hesitate to contact physicalsecurity@wiz.io and/or your HR business partner at askhr@wiz.io for assistance.

In the event of a lost or stolen laptop or mobile device containing Wiz data (including email), you should notify your supervisor and the IT team (it@wiz.io) immediately. If you can't report from your Wiz email address, use the personal email address that Wiz has on file from your onboarding process (IT will verify your identity).

If the device has been stolen, report the incident to your local law enforcement authorities and provide them with all the necessary details. IT or the Corporate Security team can provide laptop serial numbers, model information, etc. as needed. Policy report numbers, law enforcement contact information, etc. should be provided to IT and/or Corporate Security upon request.

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.

Alert the information security team immediately via phishing@wiz.io or the #phishing Slack channel 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.

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.

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 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.

Emailing and communicating sensitive data or files to external recipients doing business with Wiz: This is acceptable in the ordinary course and for purposes of legitimate Wiz business. Wiz provides **its personnel** with tools and procedures to securely share files with authorized recipients. You should not e-mail data or files that contain sensitive information to external recipients unless it is expressly permitted as part of an existing relationship with a customer, vendor, or partner, or otherwise if 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. If you need assistance using Wiz tools to securely send information, please open a ticket with the IT team.

Emailing and communicating sensitive 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.

8. Use of Instant Messaging

Slack is the authorized instant messaging service at Wiz. You should use Slack 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
- You should only share information with Wiz Personnel who have a need to know that information
- You should only communicate business sensitive information via direct message (1:1 chatting) or in closed groups, NOT in any general or public company channels
- Do not share any Wiz customer platform findings via Slack (including screenshots)
- Do NOT upload customer files, tenant screenshots, or other customer data to Slack

External Slack connections (i.e., with customers) may be established for business purposes. Connecting with external Slack users for personal conversations is prohibited.

Other instant messaging services (e.g. WhatsApp) for business communications or to share any confidential information relating to Wiz or its customers.

Wiz personnel may attend meetings hosted by customers or partners on third-party services such as Microsoft Teams or Google Meet. However, these services should not be used for instant messaging outside of the scope of meeting events. Exceptions to this policy may be approved on a case-by-case basis. To request an exception, email it@wiz.io. Approval from your manager and from Security will be required.

9. Monitoring of Wiz IT Systems

Wiz monitors Wiz IT Systems and sometimes accesses information stored on or communicated through those 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 compliant with Wiz's policies and procedures and does not pose a risk to Wiz's compliance, legal standing, or business interests.

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. If you are using a Wiz-managed web browser, URLs you visit may also be logged. This information is processed in accordance with local laws and regulations. **As explained above, for this reason, we recommend that you do NOT store personal / private information on your Wiz computer, drives, or other Wiz IT Systems or Hardware.**

Monitoring may be conducted in the following ways:

- General and continuous monitoring: In most cases, this type of monitoring will be automated (e.g., 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: The Wiz 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 of Wiz IT Systems or your Wiz email account and/or to access your Wiz Hardware, we will take steps to discuss with you beforehand 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 and/or sales teams to collect performance data or to monitor and improve user service and sales.

Monitoring of your Wiz email account and calendar: Wiz or its third-party service providers may implement automated monitoring and

analysis capabilities for e-mail and calendar entries associated with sales activity for the purposes of monitoring and improving sales performance.

11. Clean Desk & Clear Screen

Wiz maintains a clean desk and clear screen policy. Clear desk and clean screen practices ensure that sensitive information, in both digital and physical formats, is not left unprotected nor unattended in personal or public workspaces. Clean desk and clear screen practices include:

- Removing confidential documents or paperwork from your desk/workspace when you leave the area (either take them with you or secure in a locked cabinet).
- Lock your computer screen every time you walk away from your desk.
- Using a laptop privacy screen when working in public areas.
- Erase sensitive information from any whiteboards or other publicly visible area.
- Removing papers from printers immediately.
- Shredding sensitive documents.
- Removing personal items from your desk/workspace at the end of each working day.

12. Password and Credential Management

Wiz utilizes Okta for Single Sign-On (SSO) access to all authorized SaaS applications and services, and 1Password Enterprise as its approved password manager for all other cases where standalone passwords, secrets, or other credentials must be stored and accessed. Wiz personnel must adhere to guidelines provided by the IT and Information Security teams when using these services. Wiz personnel must not use systems other than Okta or 1Password for storing user credentials.

13. External Services

All Wiz Personnel are required to ensure no Wiz confidential data is shared with external services unless they have been specifically authorized by Wiz's Procurement team. External services include, but are not limited to, AI-based systems like ChatGPT, browser extensions like Grammarly, file storage and sharing services like iCloud and/or Dropbox, note-taking services like Evernote, and social media. Wiz Personnel 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.

14. Social Media

Wiz Personnel are responsible for content they publish on social media and can be held personally liable for content published. Many

social media services (e.g., LinkedIn, X) blur the lines between business and personal. Keep this in mind and please consider both your professional reputation and Wiz's reputation when crafting your posts. If you manage social media as a part of your Wiz job duties, ensure you are separating your Wiz accounts and your personal accounts.

Do not post any financial, confidential, sensitive, or proprietary information about Wiz, our partners, or our clients. Wiz Personnel can be subject to disciplinary action for publishing inappropriate or classified content.

This Policy cannot cover every scenario related to social media. Use your best judgment and ask your manager for guidance if needed.

15. Handling Customer Information

Customer information should be protected as rigorously as internal Wiz information. Specific activities, such as sharing customer platform findings via Slack or recording screenshares/video calls within customer environments, are specifically restricted.

Customer data must never be stored locally on laptops.

Wiz access to customer tenants: Customer consent is required to create user accounts for Wiz Personnel. Wiz Personnel accounts on customers must be:

- Limited to the SE or CSA team members directly supporting the customer.
- Granted minimal privileges needed for reporting or troubleshooting.
- Managed through Cognito.
- Configured with unique passwords, not re-used across tenants.
- Removed when no longer required.

If you have any questions on how to better protect customer information, email security@wiz.io or reach out to the #ask-security-privacy-compliance channel on Slack.

16. Policy Exceptions

We expect compliance with all Wiz policies. If your compliance is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, Wiz Personnel must request an exception by emailing GRC@wiz.io and following the steps requested. Exceptions will be approved on a case-by-case basis and their approval is not automatic. Exceptions that are granted will be for a specific period of time, not to exceed one year. Upon expiration of the exception, an extension of the exception may be requested, if it is still required.

17. Related Documents

Purchasing Policy (WorkRamp)

Wiz Mobile Device and Applications Management Policy

18. Document Ownership and Approval

18.1 The Chief Information Security Officer (CISO) is the owner of this document.

18.2 This policy is designated as critical; the CISO is responsible for ensuring the policy is reviewed and approved annually.

18.3 The current version of this document is available to all staff on the internal policy management tool.

18.4 This policy was approved by Ryan Kazanciyan, CISO and is issued on a version-controlled basis.