ROGERS

Privileged & Confidential – Legal Advice

From: Megan MacDonald, Director, Regulatory Counsel
Date: March 4, 2025
Re: GitHub Copilot Guidelines and Requirements

PLEASE READ FULLY AND CAREFULLY.

Your ability to retain or obtain a GitHub Copilot license depends on your full compliance with each of the requirements and key steps outlined herein. Your license will be immediately revoked, without warning, in the event of non-compliance.

For any questions, please contact Megan MacDonald (megan.macdonald@rci.rogers.com).

This memorandum is confidential and intended solely for internal use within Rogers Communications Inc. ("Rogers" or the "Company"). Any external dissemination or copying is strictly prohibited.

In connection with and in exchange for your access to a GitHub Copilot license, you are required to comply with all requirements set out herein (the "**Copilot Guidelines**"), and to certify your ability and willingness to comply in accordance with the steps set out below.

Tools with artificial intelligence ("**AI**") capabilities offer significant opportunities for Rogers while also introducing or highlighting tool-specific risks. These risks must be understood and mitigated by all users to protect Rogers' interests and competitive position. These Copilot Guidelines identify areas where your continued vigilance is required from a compliance perspective to identify, address and communicate potential risks related to the use of GitHub Copilot at Rogers.

Acceptable Use of AI at Rogers

1. Principles of Responsible AI Usage

- To ensure Rogers' use of GitHub Copilot advances Rogers' business interests in an ethical and secure manner in accordance with Company values, you are required to adopt a risk management focus for all GitHub Copilot-related use, always focusing on identifying, assessing, mitigating, and monitoring known and unknown risks in accordance with these Copilot Guidelines.
- All use of and reliance on GitHub Copilot must be guided by the following principles of responsible AI usage:
    - Safety and Security
    - Data Protection and Privacy
    - Ethical Use and Accuracy
    - Transparency
    - Monitoring
- **YOU WILL** immediately flag any new, unusual, or previously unidentified risks, ethical concerns, security issues, or other suspected violations of these Copilot Guidelines to

ai_risk@rci.rogers.com or Rogers STAR hotline.

2. **Safety and Security**: The use of GitHub Copilot could increase the risk of a threat actor gaining access to or compromising sensitive code or data via the GitHub Copilot tool if your device or account is breached, whether technologically (hacking, phishing, malware, data poisoning[1], prompt injection[2], *etc.*) or physically (unlocked devices, exposed passwords, *etc.*).

- **YOU WILL** exercise a high level of caution to prevent physical and technological security breaches of any corporate account or device while assigned a GitHub Copilot license.

3. **Data Protection and Privacy**: GitHub Copilot is contained within the Rogers tenant and Microsoft is restricted from using Rogers-specific inputs and data to train its broader AI models. Other AI tools not explicitly approved by Rogers do not offer these protections and must not be used.

- **YOU WILL NOT** enter Company information into any unauthorized AI tool.[3]

- **YOU WILL NOT** use the "Everyone except external users", "People in Rogers Communications Inc.", "Everyone at Rogers", or any equivalent or broader setting to grant access to any files or folders containing any code created with the assistance of GitHub Copilot.

- **YOU WILL** take all necessary steps to ensure that your use of GitHub Copilot does not result in the unauthorized disclosure of Personal Information[4] or other sensitive information to: (i) other Rogers employees who should not have access to it; (ii) the public; or (iii) any other unauthorized third party.

4. **Ethical Use and Accuracy:** The use of AI applications, including GitHub Copilot, carries potential risks arising from how AI applications work, including potential errors in output, AI hallucinations (where AI presents information that has no basis in reality), lack of consistency in output results, lack of transparency in how AI output is produced, and ethical considerations such as bias, misinformation, and deep fakes. Be aware that AI-generated code can reflect biases present in the training data and may contain errors or bugs. GitHub

---

[1] A form of cyberattack by which an attacker seeks to compromise the integrity or performance of an AI System by deliberately introducing false or misleading information into the data used to train an AI System.
[2] A form of cyberattack by which an attacker seeks to manipulate an AI System into disclosing sensitive information or engaging in unauthorized or unethical activity by injecting malicious prompts or commands into the AI System, often in the form of seemingly benign input.
[3] Note that you are prohibited from sharing Company information with publicly available third-party AI systems and applications unless you have been granted explicit permission to do so.
[4] Personal Information is any data or information that could identify a particular person. Examples include a full name, Social Security number, driver's licence number, bank account number, passport number, and email address. See ISEC 4 Data Governance.

Copilot may generate code that seems plausible but is incorrect or nonsensical.

- **YOU WILL** be mindful that GitHub Copilot is a tool intended to assist you, and not replace you.

- **YOU WILL**, prior to relying on any code generated by GitHub Copilot for business purposes:

    - Apply your judgment, expertise, and critical thought to fact-check and "sense-check" the code to ensure that it:

        - Is fair, unbiased, and functions correctly; and

        - Does not improperly use or disclose sensitive information, including Personal Information;

    - Review and test the code to ensure it meets your project's standards and requirements; and

    - Cross-check the code against reliable sources and/or documentation to verify its accuracy and relevance.

- **YOU WILL NOT** use or attempt to use GitHub Copilot to avoid or bypass any policy, law, rule, or regulation binding you or Rogers, or to mislead, deceive, manipulate, or exploit any Rogers employee, Rogers customer, or other impacted stakeholder.

5. **Transparency:** A lack of transparency regarding your use of GitHub Copilot for business purposes could jeopardize your and the Company's ability to (i) make ethical and responsible decisions, (ii) comply with disclosure obligations, (iii) attest to the accuracy and truthfulness of corporate and accounting Records on behalf of the Company, and (iv) comply with laws related to privacy and intellectual property (i.e., copyright, trademarks, and patents).

- **YOU WILL** be transparent regarding all use of and reliance on GitHub Copilot for business purposes when asked.

- **YOU WILL**, whenever you rely on GitHub Copilot as a co-developer, whether in whole or in part, clearly and conspicuously mark any resulting work product with a statement sufficient to alert any user or other impacted stakeholder of the extent of your reliance on AI-generated code and any associated risks (an "**AI Declaration**").

    - **Sample AI Declaration:** An acceptable AI Declaration will be tailored to reflect

your specific reliance on and use of GitHub Copilot, including a high-level description of any steps taken to mitigate the AI-related risks identified in these Copilot Guidelines. By way of example only, an acceptable AI Declaration could include the following:

- "Portions of the code in this repository were generated by AI tools, including GitHub Copilot. All AI-generated code has been reviewed and tested to ensure it meets project standards and requirements."

- **YOU WILL** prominently display the required AI Declaration in one or more of the following locations:
  - The root page of your repository (e.g., in the README.md file, "About" section, or similar);
  - Your CONTRIBUTING.md file; and/or
  - A section in your CODE_OF_CONDUCT.md file.
- **YOU WILL NOT** attempt to conceal your reliance on GitHub Copilot or pass off content generated by GitHub Copilot as your own work product.
- **YOU WILL NOT** delegate responsibility to GitHub Copilot, directly or indirectly, for verification of the accuracy or completeness of any information required by the Company to comply with any applicable law, rule, or regulation without clearly and conspicuously disclosing that delegation to all relevant stakeholders.

6. **Monitoring**: Outputs from AI tools must be continuously monitored, evaluated, and improved to identify, measure, and mitigate risks and unintended outcomes. As a GitHub Copilot user, Rogers requires your assistance in identifying, measuring and assessing potential risks associated with the GitHub Copilot tool. Rogers also reserves the right to monitor your use of the GitHub Copilot tool as reasonably required to protect its business interests and meet its legal obligations.[5] You should have no expectation of privacy in connection with any aspect of your use of the GitHub Copilot tool.

- **YOU WILL** take immediate action to report any identified biased, unethical, or discriminatory GitHub Copilot output, as well as any GitHub Copilot output demonstrating a trend or pattern of errors that cannot be corrected through improved

[5] Including, for example, to ensure compliance with these Copilot Guidelines, monitor workplace performance, ensure compliance with privacy and intellectual property laws, *etc*.

queries, to EnterpriseDevOps1@rci.rogers.com or Rogers STAR hotline.

- **YOU WILL** be alert to any potential security vulnerabilities in the code generated by GitHub Copilot, and regularly perform security audits, using appropriate tools to identify and fix identified issues, in addition to flagging concerns to EnterpriseDevOps1@rci.rogers.com.
- **YOU WILL** be mindful that all code generated by GitHub Copilot, as well as all associated inputs, prompts, metadata, and AI Declarations, could become the subject of disclosure in legal proceedings and regulatory investigations.
- **YOU WILL NOT** use GitHub Copilot to directly or indirectly do anything you are prohibited from doing by any Company policy, law, rule or regulation, and will ensure that otherwise lawful conduct does not become suspect because of a poor choice of words.
- **YOU WILL** be mindful of potential copyright issues when requesting that GitHub Copilot generate generic solutions, and craft specific and purpose-built prompts to minimize risks of copyright infringement, as required.[6]

* * *

To confirm that you have received a copy of these Copilot Guidelines and that you have read them, understood them, and agree to comply with them, please complete the form available at Acceptable Use of AI at Rogers – GitHub Copilot Guidelines – English.

* * *

[6] Please note that, to help prevent against risks of copyright infringement at the enterprise level, suggestions that match public code are filtered to prevent duplication. As such, developers may receive notifications indicating that a suggestion cannot be provided due to this filter.