Orion Software Code Usage Policy

Policy Statement

All Orion employees subject to handling code, must strictly adhere to this policy. The policy prohibits storing ,Sharing or copying Orion's code to public repositories, personal devices, or unauthorised cloud services. Violation of this policy will result in serious disciplinary action, including termination and or legal action if necessary.

Risks with Public Repositories

1. **Reputation Damage**: Storing code in public repositories is a huge risk. A security incident related to a data leak from a public repository can severely damage Orion's reputation and weaken's client trust.
2. **Compliance Issues:** Sharing code publicly breaches licensing agreements ,regulatory requirements and client confidentiality obligations
3. **Intellectual Property Theft**: Unauthorised access to Proprietary code or innovative solutions hosted in the public domain will violate intellectual property rights. (can be copied, viewed and downloaded by others. This is violation of intellectual property rights.)
4. **Exposure of Sensitive Data**: Accidental inclusion of sensitive information like credentials, API keys, client proprietary code or access token in in public repository can result in security breaches which leads to data exfiltration and financial losses for Orion. (can lead to security breaches.)
5. **Malicious Contributions:** Attackers can submit compromised or backdoor malicious code via pull requests, which, if not properly reviewed, can introduce security vulnerability and compromise your project.
6. **Secrets Exposure**: Public repositories often contain cloud secrets like API keys and access tokens, which leads to data exfiltration and financial losses for Orion.(this point is merged with Point 4)

How can we Avoid these Risks.

1. **Use Orion Approved Code Repositories: Always** Store all source code in Orion approved tenants / repositories. (e.g., Orion licensed - GitHub Enterprise, GitLab, Azure DevOps etc.).
2. **Do Not Upload Proprietary Code**: Ensure no Orion or client proprietary or sensitive information is included in any code uploaded to public repositories.
3. **Seek Approval**: All Orion employees requiring access to public repository for legitimate business need to submit an request with Orion Helpdesk ticket with business justification along with approvals from respective projects manager and delivery heads. The request will be reviewed and approved by Orion Global compliance / Orion IT and access will be provided to Orion licensed repositories
4. **Registering with Orion email ID's:** Do Not use Orion email ID's in accessing unapproved public repositories (e.g. Anaconda, WeTransfer etc.). Unauthorized registrations will pose security risks and exposes company data to external tracking
5. **Secure Development Environments: Always** use company provided devices and accounts for all development work. Avoid saving code on personal computers, USB drives, or cloud storage (e.g., Google Drive, Dropbox, OneDrive).

Consequences for Policy Violations

- Employees in violation of this policy will face disciplinary actions, including possible termination. Legal consequences may be pursued depending on the severity of the violation.
- The company reserves the right to take necessary action to protect its intellectual property and client confidentiality.

Acknowledgment and Agreement

I acknowledge that I have read, understood, and agree to comply with this Policy. I understand that storing company code in public repositories is strictly prohibited and that violations will result in serious disciplinary actions.