AppShark

Code Security Process

Important points to be considered for Code Security Process:

1. The walk through sessions about the Code Security process need to be conducted during the following phases:
    a. **Induction stage** – As part of induction program we need to ensure that the code security process should be covered to the new hires.
    b. **Regular Awareness Sessions** – Frequent sessions/reminder emails should be conducted / sent so that employees are well aware of the Code Security Process along with SVN. How to use SVN will be rolled out by the respective PM's and in case of any further clarifications they can reach out to Technical Leads/IS teams. Once training is done, it is mandatory for all employees to acknowledge the session through an exam conducted by the session owner.
    c. **Project Kick off stage** – It is the PM's responsibility to ensure that as a part of project kick off we need to let the project team know once again about the process that we are following with respect to code security's, Do's & Dont's.
    d. As part of reminder, PM once in a sprint cycle during the stand-up meetings need to emphasize the importance of code security.
2. Any other code repositories apart from SVN which are maintained for the project need to have approval from the Account Manager.
3. If anyone needs access, they need to approach IS Team through proper approval mechanism. Access to specific source control tools like Github, Bitbucket etc will be provided to specific technical panel team members who fall under technical lead roles and with proper approval mechanisms.
4. Any violation by the resource will be strictly considered as non-compliance and considered to be breach of conduct.
5. All signed acknowledgements (Hard copy & Scanned copy) need to be collected by HR and secure in repository.

6. Please note that in case of any Customer specific projects where code security is considered to be strictly complied, we need to ensure that the project team engaged for the project, not supposed to access the code from unapproved IP addresses. Same can be access through VPN's under proper approvals from the respective PM.
7. Any non-compliance by the resource regarding Code Security will be strictly considered as Security breach and lead to termination of employee with immediate effect.

Note:

Any Non-Compliance in terms of Code Security, it is the responsibility of the PM to ensure that we follow the Code Security right from beginning of the development till end the of the project delivery.

He / She should educate the project team with respect to confidentiality, integrity and availability of the code in the project folder / SVN.

Do and Don’ts for Code Security

Do’s:

- Be aware of data sensitivities and handle floor with care.
- Follow IT Assets undertaking policy and sign the relevant documents if you are using an official IT asset.
- Follow the SVN’s process which will be rolled out by session owners.
- Daily check-in’s need to be done in SVN’s whenever there is a development activity\changes performed and the same need to retrieved from the repository when you restart the dev work for the project.

Don’ts:

- We are not supposed to upload the code in public folders, pen drive, email etc.
- Do not push any secured information into repositories like user name & passwords of integrations, authentication keys etc.
- Do not access Customers related sites from the IP’s which are not permitted by the Customer.
- Do not access/send project related code to outside other than AppShark domain.
- Not supposed to take any code snapshots through mobiles.
- Once the project is completed we are not supposed to store the code in the local repositories and the same need to be ensured by PM as part of project closure process.