Secure Development Policy

1 INTRODUCTION

1.1 Purpose:

The purpose of this document is to establish responsibilities of development team of Sybrid PVT LTD for Secure Application development and code standards.
Developers must consider security as part of their common coding practices.

This policy shall reduce:

1. The likelihood of malicious code will be inserted in software.
2. The impact of malicious code that is already present in deployed software.

1.2 Scope

This policy is applies to all developers of Sybrid Private Limited.

2 POLICY

The adherence to and use of Secure Application Development Coding Policy is a requirement for all software development in Sybrid PVT LTD.

HOD or senior software engineer will lead the development of code and validate with the most current standards for secure application development.

Only validated code will be implemented into the production environment by the Sr. Software Engineer or HOD.

Development environment will be separated and access will only be allowed to the authorized developer to ensure the information security requirements.

Guidance will be given by HOD or Sr. Software Engineer to ensure the security of software development and their codes against each programming language.

Developers must ensure the following while development of any software/module/workflow

- Input Validation
- Authentication and Password Management
- Session Management
- Access Control
- Cryptographic Practices

- Error Handling
- Data Protection
- System Configuration
- Database Security
- Memory Management
- General Coding Practices

The developer will refer to “Roles and security” in requirement gathering form to protect the data and information during the designing phase.

Development, UAT, Production all environments will be separated with their security check and balance, HOD will ensure the access generation accordingly.

Version controlling will be implemented by TFS server and senior software engineer will be responsible for version controlling.

Developer to apply all security checks to restrict fraudulent transaction, defaced application, orphan user accounts and will also ensure audit trail(s) for user access in all developments.

Relevant authorized user should be well aware of the security measures in the respective application they are using.

Developer must have knowledge to deal with the possible vulnerabilities and weaknesses while developing the required program.