CCB CORPORATION
WEB APPLICATION SECURITY POLICY

1. Purpose

This policy provides a framework for the management of web application security throughout CCB Inc. Information is an essential asset to CCB Inc., so nonpublic information of CCB Inc. should be protected. Web application assessments are performed to identify or realized weaknesses because of weak authentication, insufficient error handling, and sensitive information leakage. To mitigate these issues will reduce the possible attacks on both internal and external services, and therefore enhance the information integrity, confidentiality, and availability of CCB Inc.

The policy describes the web application security requirements that CCB's employees, guests, contractors, third party personnel, and consultants should follow. The policy defines protective measures for all web applications that the company used.

2. Person Affected

CCB's employees, guests, contractors, third party personnel, and consultants.

3. Policy

The policy of CCB Corporation is to ensure:

3.1. Access Control

a. Use individual username and password to access network, servers and applications.
b. General or Group IDs should not Normally be permitted.
c. User IDs and passwords are required to gain access to CCB's networks and applications. Password issuing, strength requirements, changing and control will be managed through formal processes. Passwords setting requirements are listed below:
    - Use a minimum of 8 characters.
    - Must contains at least an uppercase and a lowercase character.
    - Must contains at least a number.
    - Must Contains at least a non-alphanumeric character.
    - All passwords will be expired every 90 days.

d. The user's access rights and privileges must be limited to perform only tasks that the user is authorized and not beyond his authority. Where possible no one will have full rights.
e. Applications must prevent users from directly accessing internal objects, API's, files, and databases. The application must interact on behalf of the user.
f. All built-in user IDs, testing user IDs, and IDs with default passwords been removed from the operating system, web servers and application itself before final production.
g. Employees' logon IDs will be terminated after they resigned.

3.2. Secure Coding

a. Validate all input parameters to prevent attacks.
    - CCB should ensure that all parameters in the company have to be validated before they use it.
    - The programmers in CCB develops a centralized module to process input parameter validation.
    - The company need to check which types of the input will be allowed and whether the parameter is required or not.
    - The programmers should make sure the minimum and maximum length of expected set of characters that can be accepted in the application.
b. Sanitized application response.
    - Develop a centralized module that any sanitization should the performed.
    - All output, return codes and error codes from calls should be checked to ensure that the processing expected actually occurred.
    - Some unnecessary internal system information which is from the internal servers during a response can not be appeared in the client side.
c. HTTP trust issues.
    - Programmers should not believe and depend on HTTP REFERER headers, form fields or cookies to make security decision.
    - CCB cannot believe the hidden parameters cannot be changed by the users, because hidden parameters can be easily affected by attackers.
d. Keep sensitive values on the server to prevent client-side modification
    - Can not put any sensitive information in client browser cookies.
    - Programmer should use strong cryptographic techniques to safeguard the confidentiality and integrity of the data.

3.3. Antivirus

a. Corporate files servers and workstations will be protected with virus scanning software.
b. Virus update patterns will be updated regularly on corporate servers and workstations.
c. All drive and disk (USB, cd-drive) which brought in from outside of corporation is forbidden to be used.

3.4. Prohibited Activities (You can't do)

a. Open any unexpected Email and any attachment.
b. Use of any external proxy systems or other similar technologies.
c. Use of non-standard remote control technologies.
d. Install personal or unauthorized web applications.

4. Definition

Confidentiality:
Information should not be made available or disclosed to unauthorized individuals, entities, or processes.

Integrity:
The act of safeguarding the accuracy and completeness of assets.

Availability:
Information should be accessible and usable upon demand by an authorized entity.

Access control
The process of limiting access to the resources of a system only to authorized programs, processes, or other systems.

Password
A protected, private character string used to authenticate an identity

Virus
Computer software that replicates itself and often corrupts computer programs and data.

5. Policy Compliance

Responsibilities

a. All employees of CCB are required to adhere to the Web Application Security Policy and assist the process and procedure of the policy.

b. Information Security Manager leads the design, implementation, operation and maintenance of the web application security management system based on the policy. In addition, information security manager leads monitoring to ensure compliance both with internal web application security policy and application laws and regulations.
c. Department of Information Management and Technology provides web applications support and information technology solutions including designing, installing, and maintaining various computer networks.
d. Information Technology Committee reviews web application performance and monitors technical developments according to the web application security policy.

6. Revision History

Date	Revision No.	Change	Ref. Section
09/30/2015	1.0	New policy drafted	
10/01/2015	1.1	Adding password requirements	3.1.c
10/06/2015	1.2	Adding prohibited activities	3.4