ANNEX "C"

SECURITY REQUIREMENTS

ARTICLE I
Technical Security Requirements

1. In order to access credit data from the CIC, Accessing Entities (AEs) should have the following technical security requirements which are applicable to all AE's information assets that will be used to obtain, process, store, and release data from the Credit Information System (CIS):

    a. Internet connection with at least 1MB upstream.
    b. FTP Client or internet browser software installed with Transport Layer Security (TLS) 1.2 support.
    c. Latest Gpg4Win encryption software installed.
    d. FTP account and server information obtained from CIC.
    e. FTP servers public gpg key obtained from CIC.
    f. Anti-Virus software installed and updated on equipment where access is to originate.
    g. Registered to the CIC all public IP addressed where access is to originate.
    h. Configured corporate firewall to allow connection to CIC servers:
        a. Server IP addresses: 202.90.128.58 to 202.90.128.62
        b. Service ports (TCP): 21, 443, & 65000-65100
    i. The system of the AE should have any of the following supported platforms: Windows 7/8.1/2008/2012, Mac OSX, & RedHat/Ubuntu Linux

2. Other Provisions:

    a. The purpose of this Agreement is to provide a checklist that allows for self-declaration of an AE to its commitment to adhere to the guidelines herein. The AE must be ready to submit to the CIC, proof that such recommended activities, or its relevant equivalent as determined by the AE, is being implemented.

    b. CIC reserves the right to improve, modify, add, or remove, in part or as a whole, provisions in this document as the security environment, globally and locally, change.

ARTICLE II
Information Security and Privacy Programs

The AE agrees to establish an information security program to ensure that Data Subjects' credit data from the CIC have adequate protection from unauthorized alteration and disclosure. Likewise, the AE agrees to abide by the requirements of the National Privacy Commission (NPC) to ensure privacy of Data Subjects' personal data and adequate protection from the same security risks. The AE shall adopt the following security best practices to achieve the following objectives:

a. Establish a formal written information security and data privacy policies.

b. Identify and define the roles and responsibilities for the protection of CIS data and for carrying out specific information security processes.

c. Designate an individual or individuals that will be responsible for the protection of personal information especially Data Subject's credit and personal data from the CIS.

d. Designate an individual or individuals who shall be accountable for ensuring compliance with applicable laws and regulations pertaining to data privacy, security, and valid use of credit data.

ARTICLE III
Information Security and Privacy Awareness Training

The AE agrees to provide security and privacy awareness training to their employees that will be involved in the processing of Data Subjects' credit and personal data from the CIS, to ensure the latter are aware and understand their responsibilities, and exhibit the necessary behaviors and skills to protect those data from security risks, by ensuring that:

a. Employees are aware that credit information of Data Subjects accessed from the CIS shall only be used for the purpose of establishing the creditworthiness of the Data Subject.

b. Employees have the necessary training on the importance of enabling and utilizing secure authentication methodologies. Likewise, have the necessary training to identify and properly store, transfer, archive and dispose sensitive information.

c. Employees have the necessary training on how to identify different forms of privacy threats such as social engineering attacks, viz. phishing, phone frauds and impersonation calls.

d. Employees have the necessary training to be able to identify the most common indicators of an incident and be able to report such an incident to the appropriate person.

e. Maintain list of employees handling, viewing, or using CIC data with certification to the effect that they have received the above training.

ARTICLE IV
Access Management

The AE agrees to establish a formal registration and de-registration procedures to ensure that only authorized personnel is granted access to credit and personal data of Data Subjects from the CIS, to protect those data from unauthorized access and use, and ensuring the following:

a. Restrict access to credit data only to personnel with appropriate security clearance granted by its management.

b. Enforcement of secure password policy to employees to protect their credentials from disclosures. Likewise, comply with the secure password requirements of the CIS.

c. Restrict access to credit data only from authorized application systems and computer hosts.

d. Use of encryption and multi-factor authentication methods when accessing credit data online.

e. Enforce access to information stored in file systems, network shares, applications and databases that process Data Subject's credit and personal data, only to authorized users and with the need to access the information as a part of their responsibilities.

ARTICLE V
Data Security Measures

The AE agrees to protect credit and personal data of Data Subjects from intentional or unintentional security events to avoid adverse impact on CIS data subjects from risks, and shall observe and perform the following:

a. Encrypt credit and personal data of Data Subjects when storing on any physical media such as hard drives, USB drives, CD/DVD, among others.

b. Do not use fax machines to transmit documents containing credit and personal data of Data Subjects*.*

c. Transmit credit and personal data of Data Subjects only on networks with adequate protection.

d. Store and process credit and personal data of Data Subjects on computer host with adequate anti-virus or malware protection.

e. Backup media of credit and personal data of Data Subjects are adequately protected when stored and transferred across the network or physical location.

f. Dispose properly all computer or media where credit and personal data of Data Subjects were processed.

g. Ensure that credit and personal data of Data Subjects are not shared to business units or business partners located outside the Philippines.

ARTICLE VI
Host and Network Security

The AE agrees to establish guidelines for IT security and to communicate the controls necessary to maintain a secure network infrastructure. Said guidelines must support the mechanisms to protect confidentiality and integrity of credit and personal data of Data Subjects.

a. Change all default passwords before deploying new information assets on production network.

b. Allow only vendor supported, updated and stable software esp. web browsers and email clients in production network.

c. Configure end-point security solutions to automatically conduct an anti-malware scan of removable media when inserted or connected to computers.

d. Configure end-point security solutions or operating systems to disable the auto-run feature for removable media.

e. Configure all computer hosts to deny all incoming traffic except authorized network services.

f. Lock workstation sessions automatically after a standard period of inactivity.

g. Allow only authorized network services on the network.

h. Enable local logging or centralized logging on all hosts and networking devices.

i. Use DNS filtering services to help block access to known malicious domains.

ARTICLE VII
Vulnerability Management

The AE agrees to identify, assess, and remediate security vulnerabilities in their IT assets to prevent unauthorized users from exploiting such weaknesses to gain access to AE's information processing systems. This activity involves identifying IT assets, assessing vulnerability of those assets, and remediation of issues found in those assets.

a. Deploy an automated system update solution in order to ensure that the operating systems and applications are running the most recent security updates provided by the software vendor.

b. Conduct regular external and internal penetration tests to test the overall strength of the corporation's defense, identify vulnerabilities and attack vectors that can be used to compromise corporate information assets.

ARTICLE VIII
Information Security Incident Management

The AE agrees to establish a consistent approach to manage information security incidents, including communication of security events and weaknesses that may have adverse impact on the confidentiality and integrity of credit and personal data of Data Subjects from the CIS.

a. Upon detection report all information security incidents affecting the access of credit and personal data of Data Subjects to the CIC Information Security Unit: infosec@creditinfo.gov.ph.

b. Establish a written incident response plan that define roles of personnel as well as phases of incident handling/management and communicate the same to all parties involved.

c. Designate management personnel, as well as his/her alternate, who will support the incident handling process by acting in key decision-making roles.

d. Maintain contact information of as relevant government agencies and law enforcement to report information security incidents.

e. Publish information for all employees on reporting information security incidents to appropriate authority within the organization.

ARTICLE IX
Third-party Security

The AE agrees to adopt security best practices when dealing with suppliers and contactors. The AE must ensure that their suppliers and contractors will abide by AE's information security policies or the third-party must be able to demonstrate their own corporate security policies providing equivalent assurance such as:

a. Complying with this CIS access security requirement.

b. Access to credit data from the CIS is governed by strict procedures.

c. Data sharing agreements complies with the requirements of the NPC.