Acceptable Use and Legal Policies Agreement 2019-2020

This is a LEGALLY binding contract. Any violation of this contract may be prosecuted by the full extent of the law. By signing this document, you agree that you may be held responsible for any actions that are included in this document but not limited to: internet policies, server-side policies, and/or any other potential policies that the company has provided. This server is intended NOT to be used for malicious intent, by the signatory of the document.[1] All activities on the server is logged and monitored. Any unauthorized attempt to gain access to the server may result in legal prosecution.

ACCMS Solutions solely provides the hosting of the server for its contractors and employees, and the policies may not be altered unless stated otherwise.

By signing this contract, you agree to the conditions that are outlined in this document and policies in the following pages.

Print Name (CLEARLY): _____

Signature: _____

Date:_____

[1] If this server is used for malicious intent, the signee must assume all responsibility, even if damage has occurred and/or the damage wasn't caused by the signee.

The following outlines the purpose and proper use of the server. Anything outside of the following scope is against the company's policies. These policies are in match with the *ACCMS Solutions Acceptable Use and Legal Policies Agreement 2019-2020.*

BEGINNING OF POLICIES

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by ACCMS Solutions. Effective implementation of this policy will minimize unauthorized access to ACCMS Solutions proprietary information and technology, and to establish a baseline order for acceptable use.

2.0 Scope

This policy applies to server equipment owned and/or operated by ACCMS Solutions, and servers registered under any ACCMS Solutions-owned internal network domain.
This policy is specifically for equipment on the internal ACCMS Solutions network. For secure configuration of equipment external to ACCMS Solutions on the DMZ, refer to the Internet DMZ Equipment Policy.

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at ACCMS Solutions must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Administrators.
Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Administrators.
• Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
o Server contact(s) and location, and a backup contact
o Hardware and Operating System/Version

o Main functions and applications, if applicable
• Information in the corporate enterprise management system must be kept up-to-date.
• Configuration changes for production servers must follow the appropriate change management
procedures.

Only those who are priviledged may access the files/areas on the server. Those who lack these privileges cannot access those certain files/areas. Failure to comply will result in the disiplinary action (See 4.0 Enforcement)

3.2 General Configuration Guidelines

• Operating System configuration should be in accordance with approved Administrators guidelines.
• Services and applications that will not be used must be disabled where practical.
• Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
• The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
• Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
• Always use standard security principles of least required access to perform a function.
• Do not use root when a non-privileged account will do.
• If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
• Servers should be physically located in an access-controlled environment.
• Servers are specifically prohibited from operating from uncontrolled cubicle areas.
• All passwords must follow the server guidelines when creating a password. The guideline is prompted to the user and if the password field doesn't match the guidelines, the account will not be created until the guidelines are met.
• Do not reuse passwords with the account on the server and/or from any other services that can be placed in a combination list and tried on our servers.
• Creating multiple accounts or "Multi-Accounting" is prohibited, and if detected, all accounts will be banned and your IP address will be blacklisted.

3.3c Monitoring

• All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
o All security related logs will be kept online for a minimum of 1 week.
o Daily incremental tape backups will be retained for at least 1 month.

o Weekly full tape backups of logs will be retained for at least 1 month.
o Monthly full backups will be retained for a minimum of 2 years.
• Security-related events will be reported to Administrators, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
o Port-scan attacks
o Evidence of unauthorized access to privileged accounts
o Anomalous occurrences that are not related to specific applications on the host.
o Misc. attacks, see FCC and IC3 government officials for more information regarding unauthorized attacks.
• Any attempted logins from the following countries will be automatically blacklisted, and immediately reported to the FCC and IC3: China, Russia, North Korea, Iran, Iraq, Ukraine, etc. (Only North American and some European IP addresses may be allowed into our servers). These IP address will also be automatically uploaded to Pastebin for others to view. The individuals may also be attacked for attempted unauthorized access to our server from the list, since these countries are not in North America and are we are not subject to jurisdiction/extradition under these nations.

3.4 Compliance
• Audits will be performed on a regular basis by authorized organizations within ACCMS Solutions.
• Audits will be managed by the internal audit group or Administrators, in accordance with the Audit Policy. Administrators will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
• Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. You may also be litigated to the maximum extent.

5.0 Disaster Recovery Plan
In the event of a disaster, all personnel are required to save all work when a disaster is anticipated, and/or the UPS system is tripped for the time being. In the event of a disaster and profits are cut and/or equipment damage occurs, the insurance company that is in compliance with our company will cover any occurred downtime and damage.

6.0 Definitions

Term Definition
DMZ De-militariezed Zone. A network segment external to the corporate production network.
Server For purposes of this policy, a Server is defined as an internal ACCMS Solutions Server.
Desktop machines and Lab equipment may be relevant to the scope of this policy.

7.0 Revision History
TBA

END OF POLICIES
