Computer Security Code of Conduct

Code of Conduct

This Computer Security Code of Conduct applies to any User of any CB&I AREVA MOX Services' ("MOX Services") computer system, including any network, any computer, any device, any software, or any other system component, or anyone who processes information under the cognizance of MOX Services.

Monitoring and Expectation of Privacy

MOX Services computer systems are the sole property of the United States Government. MOX Services computer systems are for authorized uses only and are provided for the processing of MOX Services and US Government information. **Users have NO EXPLICIT OR IMPLICIT EXPECTATION OF PRIVACY**. Any User, system, or file on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to Federal agencies, such as the Department of Energy (DOE), National Nuclear Security Administration (NNSA), the DOE Office of Inspector General, and law enforcement personnel. Authorized officials of other agencies, both domestic and foreign, may also be provided this information. By using a MOX Services computer system, the User consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized personnel. Any non-government computer system used to access a MOX Services computer system is subject to the same monitoring and inspection terms applicable to MOX Services computer systems. This policy is not intended to abrogate any attorney/client or work-product privilege of MOX Services or with respect to third-parties. *Note***:** All Internet usage is monitored when using the MOX Services network. All outgoing and incoming internet sites being accessed by each computer are collected for auditing and continuous monitoring purposes.

General Use

- By accessing a MOX Services computer system, User consents to permit access by an authorized investigative agency to any computer used during the period of that User's access to information on a MOX Services computer and for a period of three years thereafter.
- Users shall report any known unprotected Unclassified Controlled Information (UCI) or unprotected Classified information to the MOX Services Facility Security Officer (FSO).
- Users shall report any violation of this Code of Conduct to the FSO.
- All MOX Services information and resources shall be used in an approved, ethical, and lawful manner to avoid loss or damage to information or information technology assets, operations, image, and/or financial interest.
- Electronic communications are the property of MOX Services, considered to be business records of MOX Services, and are subject to inspection and monitoring at all times.

Initials _____

Date _____

Computer Security Code of Conduct

- Users shall avoid unwelcomed comments and communications that violate an individual's dignity and/or creates an intimidating, hostile, degrading, humiliating, or offensive environment.
- Users encountering or receiving material/messages that are fraudulent, embarrassing, profane, discriminatory, inflammatory, defamatory, hostile, degrading, overly combative, otherwise inappropriate, or illegal, shall report the incident to a supervisor, the Human Resources department, or to the Employee Concerns representative.
- Personal use of MOX Services telephones shall be reasonably brief and infrequent in nature, shall not adversely affect the work performance of the User or the User's work group, and shall create the appearance of impropriety;
- Personal phone calls to foreign countries are prohibited;
- Calls to pay-per-call services are prohibited.
- Any use of telephone recording devices or software must be approved in writing by the MOX Services Compliance or Legal Departments.
- While it is the intention of MOX Services to apply this policy uniformly and consistently, occasionally exceptions to this policy may be made when in the best interests of MOX Services.
- Users will not rely on an exception to policy granted in one circumstance or to another user as authority to violate this policy.
- MOX Services reserves the right to modify this policy at any time within its own discretion.

System Protection and Use Restrictions

Prohibited Actions

- Attempting to or gaining access to computer systems, resources, or information (this includes other user's files) for which the User is not authorized;
- Dissemination, storage, or intentional receipt or transmission of personal advertisements, solicitations, promotions, malicious software, political material or any other unauthorized use;
- Installation of any unapproved software;
- Exporting software, technical information, or encryption software or technology in violation of international or regional export control laws;
- Sharing of passwords and/or remote access PINS and tokens;
- Allowing another user to use an IT system after the User has logged on, except in authorized circumstances;
- Represent personal opinions as those of MOX Services' in any electronic communication;
- Introduction of malicious programs into the network (e.g., viruses, worms, Trojan horses, e-mail bombs, botnets, etc);
- Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type, known hoax information, rumor, or information detrimental to the reputation of MOX Services, an individual group, or any organization;

Initials _____

Date _____

Computer Security Code of Conduct

- Sending unsolicited e-mail messages, including the sending of "junk e-mail" or other advertising material (i.e., spam);
- Engaging in unauthorized use, or forging, of e-mail header information;
- Connecting a MOX Services computer system to a non-MOX Services computer or networks, except as authorized by PP14-05, *Computer Network Use* for accessing MOX Services remote access services;
- Carrying out security breaches and/or disruptions of network communication (security breaches include, but are not limited to, unauthorized data access, logging onto a system that a User is not authorized to access, disruption includes, but is not limited to, port scans, flood pings, email-bombing, packet spoofing, internet protocol (IP) spoofing, and forged routing information);
- Executing any form of unauthorized network monitoring which intercepts data;
- Circumventing user authentication or security of any host, network, system, or account;
- Unless authorized, using tools or making attempts to assess or exploit the security vulnerabilities of any system, including port or vulnerability scanning, password cracking, penetration testing, etc;
- Using and/or connecting privately-owned equipment or media (including thumb drives) to MOX Services systems (e.g., desktops, laptops, and networks) (however, personally owned head phones are permitted and commercially produced music CDs are permitted);
- Connecting any computer systems not owned by MOX Services to the MOX Services network without authorization;
- Using MOX Services computers and internet access to conduct the operations of a business other than MOX Services business (e.g., selling products or services, or running a business through another entity, such as eBay);
- Gambling in any form, including internet casino gambling;
- Accessing, sharing, sending, downloading, or viewing pornography of any kind, gambling, violence, or other objectionable or illegal material;
- Sending or forwarding e-mails that could be deemed as sexually explicit, pornographic, intimidating, harassing, or discriminating.
- Downloading and storing of information, which is not business-related on a MOX Services computer (i.e. games, software, music, videos);
- Accessing any website blocked by the MOX Services IT department using any means to circumvent the block;
- Playing computer games on MOX Services computers;
- Conducting illegal or fraudulent activities;
- Revealing or publicizing proprietary or confidential information of MOX Services, a subcontractor company, or an individual;
- Making indecent remarks or harassing or intimidating others.
- Intentionally hacking any other non-MOX Services network; or
- Facilitating any MOX Services system security breach of any type.

Audits

Initials _____

Date _____

Computer Security Code of Conduct

The MOX Services Security Department will perform system and network audits to determine if any information has been stored on individual computers or a network storage device that is not of a business nature. Non-business information will be removed immediately.

Limited Personal Use

Users are subject to DOE Order 203.1, dated 07 JAN 05, *Limited Personal Use of Government Office Equipment Including Information Technology*, states:

> "Employees may use government resources for personal purposes, but only when such use:
> a. Involves “de minimus” additional expenses to the government; and
> b. Does not interfere in any way with the mission or operations of the Department of Energy"

Users will avoid excessive personal use.

The privilege to use MOX Services computer resources for personal purposes may be limited or revoked at any time.

Information Protection

Prohibited Actions

- Transmitting MOX Services information to any individuals who are not authorized to access the information or to any systems that are not authorized to store the information;
- Violations of copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by MOX Services.

Required Actions

- Users shall comply with software licensing agreements.
- Users shall lock <Windows-L> workstations anytime the system will be physically unattended.
- Users must know the classification level and sensitivity category of information before processing the information on a computer. Users must process information only on computers approved for the information’s classification and category. If unsure of the data classification or category, Users must contact the MOX Services FSO for guidance.
- Sensitive information shall be properly protected in accordance with MOX Services’ Security policies.
- All media containing sensitive information shall be properly labeled.

Initials _____

Date _____

Computer Security Code of Conduct

- Sensitive information sent over unprotected public networks (e.g., Internet) must be transmitted only in accordance with MOX Services' Security policies.
- Password selection for all systems shall follow the password requirements as documented in MOX Services Procedure PP14-05, *Computer Network Use*.

Exceptions

Exceptions to this Code of Conduct require written approval by the MOX Services FSO.

Acknowledgement

I acknowledge that I have read, fully understand, and agree to the terms and conditions of using MOX Services computer systems contained within this Code of Conduct.

I understand that violation of this policy, no matter when occurring and whether intentional or accidental, will subject the User to administrative disciplinary action, up to and including termination from MOX Services. Additionally, there are many local and federal laws which govern computer use and Users violating such laws may be further subject to criminal prosecution. In the event that the User violates this policy and that violation causes damage to MOX Services, MOX Services has the further right to pursue civil remedies against the User.

DIPSF1 _____ DIPSF2 _____

User name (Print First, MI, Last) Company/Organization/Dept./Division

DIPSF3 _____ DIPSF4 _____ DIPSF5 _____(Y/N)

User Signature/User ID (if known) Date US Citizen

Initials DIINIT _____

Date DIDATE _____