Overview

The IT department's intentions for publishing an ***Acceptable Use Policy*** are not to impose restrictions that are contrary to all Tax Defense Network (MS) departments' established culture of openness, trust, and integrity. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of MS. These systems are to be used for *Company* business purposes in the course of normal operations. Effective security is a team effort involving the participation and support of every MS department employee and Contractor who deals with information and/or information systems. It is the responsibility of every computer user to know the following guidelines, and to conduct their activities accordingly.

General Use and Ownership

Computers and network facilities comprise all computers owned or administered by any part or connected to the Company's communication network infrastructure, including departmental computers, and the Company's computer network facilities accessed by anyone from anywhere. Authorization granted by the appropriate part of the Company's governance and/or management structure, depending on the computers and/or network facilities involved and the way they are administered.

While the IT department, Network Services Group desires to provide a reasonable level of privacy, users should be aware that the data they create on the Company's departmental systems remains the property of MS. Because of the need to protect Company's network, management will make every effort to protect the confidentiality of information stored on any network device belonging to MS.

- Users must adhere to all MS security training guidelines to avoid potential attempts by external or internal actors to introduce malicious software into the MS network.

- Users must not click on or open ANY links or attachments via email or SMS that are not from a confirmed/known trusted source.

- Users must report all suspect email, SMS, and phone calls via the Great Horn Outlook plugin where applicable and email sent to IT.

- Users are responsible for exercising good judgment regarding the reasonableness of personal use.

- Users are responsible for protecting any information used or stored in their accounts. Users shall not divulge security control information such as Active Directory user accounts, VPN and Wireless Access Points accounts, or firewall rulesets to unauthorized individuals.

- All departments that implemented research lab are responsible for creating guidelines concerning personal use of their Internet/Intranet/Extranet systems. In the absence of such policies, users should be guided by the IT department on personal use.

- The IT department recommends that any information that users consider sensitive or vulnerable be encrypted. Please consult with the IT department for guidelines on information classification and encrypting email and documents.

- For security and network maintenance purposes, authorized individuals within the IT department may monitor equipment, systems, and network traffic at any time.

- MS IT reserves the right to audit networks and systems to ensure compliance with this policy.

Security and Proprietary Information

Means should be made to classify data as either confidential or not confidential of the local controlling authority of the data (*See "Data Classification Policy" for more information)*. Examples of confidential information include but are not limited to: All MS Departmental Contractors, private data, research strategies, competitor sensitive, trade secrets, specifications, customer lists, research data and all

authorized "Third-Party clients" such as temporaries, consultants, contractors, vendors, or outside organizations who conduct business with the MS corporation. Users should take all necessary steps to prevent unauthorized access to this information. The Security and Propriety Information should be in accordance with the approved configuration guidelines below:

- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Users are responsible for the activities of their account whether they are personally executing the activity or not. System level passwords will be changed every *twelve (12) months*; user level passwords will be changed every *ninety (90) days*. Users must also conform to the IT department "*MS Password Policy"*.

- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at Five (5) minutes or less, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.

- Use encryption in compliance with the IT department's "*Acceptable Encryption Use Policy".*

- Because information contained on portable computers is especially vulnerable, special care should be exercised.

- Postings by users from the company's email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of MS, unless posting is in the course of MS business duties or has been cleared through the company's executive-level management team and/or company's head of marketing department.

- All host systems used by a user that are connected to the Company's Internet/Intranet/Extranet infrastructure, whether owned by the user or MS, shall be continually executing approved virus-scanning software with a current virus database.

- Users are responsible to report loss or compromise of their accounts to the IT department immediately upon suspicion of the account being lost or compromised. Users must fully cooperate in investigation efforts.

- Users must not leave workstations unattended and unprotected when logged into company's computing equipment. Unattended workstations must use available system mechanisms to 'lock' the workstation when the user is away. At the end of each day, the user must log out of the workstation, but leave the equipment on.

- Users are required to report any weakness in the company's computer security / any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the IT Department. If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed, the owner and the IT Department must be notified immediately.

- Remote Access to company's network facility is only permitted only under the following conditions: through the use of approved VPN account provided by the IT department and the computing system granted must have appropriate protection including anti-virus software, authentication controls, and physical protection.

- Users are required to cooperate fully with any security investigation regarding the company's equipment or systems.
- Users are required to report any illegal or unlicensed software to the IT department.
- Users are expected to read and comply with software license restrictions for any software installed in any company's owned computing equipment or any software provided or authorized

Unacceptable Use

The following activities are prohibited. Certain MS Contractors may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., network & systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is any MS Contractor or authorized "Third-Party clients" to engage in any activity that is illegal under local, state, federal or international law while utilizing the company's department-owned resources or departmental accounts. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a) Violations of the rights of any person or company protected by 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 the company.

b) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

c) A deliberate attempt to degrade or disrupt network & system performance is viewed as a violation of MS policy and/or as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.), unless this activity is a part of the user's normal job/duty and occurs within a research lab as part of an authorized procedure within that lab.

d) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

e) Making fraudulent offers of products, items, or services originating from any department account.

f) Providing unauthorized access to research data, executable code, source code, research results or partial results.

g) Effecting security breaches or disruptions of network communication. Security breaches include but are not limited to accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes. The sole exceptions to this rule are when the activity is limited to within a research lab AND authorized by the lab controlling authority, or when the IT department has given prior approval for the activity outside of a given research lab.

h) Port scanning or security scanning outside a given research lab is expressly prohibited unless prior notification to the IT department is made and approval received from the VP of IT or designee.

i) Executing any form of network monitoring which will intercept data not intended for the user's host unless this activity is a part of the user's normal job/duty or occurs within a research lab as part of an authorized procedure within that lab.

j) Circumventing user authentication or security of any host, network, or account, unless this activity is a part of the user's normal job/duty or occurs within a research lab as part of an authorized procedure within that lab.

k) Interfering with or denying service to any user other than the user's host (for example, denial of service attack), unless this activity is a part of the user's normal job/duty or occurs within a research lab as part of an authorized procedure within that lab.

l) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

m) Providing information about, or lists of, MS Contractors or users to parties outside the company’s network.

Email and Communication Activities

The following activities are strictly prohibited, with no exceptions:

n) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

o) Any form of harassment via email, telephone, SMS, or paging, whether through language, frequency, or size of messages.

p) Unauthorized use, or forging, of email header information.

q) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

r) Creating or forwarding "chain letters" or other "pyramid" schemes of any type.

s) Use of unsolicited email originating from within the *Company’s* networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by *Company’s* department or connected via *Company’s* department's network.

t) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (Newsgroup spam), mail lists or mail aliases (spam).

u) Users may not set email programs to forward or auto-forward to external email addresses.

v) The ability to access other email account does not imply a right to access those accounts. Such access may compromise confidential information and, in the case of outside systems, may lead to criminal prosecution.

w) Users are restricted from the use of email anonymizers, accounts, or any other methods of sending anonymous email messages, unless explicitly authorized for business use.

x) Users may not use unauthorized encryption software, services, or otherwise encrypt email without prior authorization from the IT Department.

Accessing or Attempting to Access Other's Files

The following activities are strictly prohibited, with no exceptions:

y) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the *Company's* departments or the end user does not have an active license is strictly prohibited.

z) Accessing, modifying, or deleting a file without the owner's permission is prohibited. The ability to access, modify, or delete does not imply permission to do so.

Software Restrictions and Use

The following activities are strictly prohibited, with no exceptions:

aa) The company requires strict adherence to software license agreements and copyright notices. Users may not make illegal copies of copyrighted material or make copies available to others. All users are responsible for compliance with copyright law and licenses for all materials including, but not limited to, software, files, documents, and graphics.

bb) Users may not download or install any unauthorized software program or utilities on any computing equipment own by MS.

cc) Users may not attempt to modify or reverse engineer licensed software or code in such a way that violates any legal agreements (copyright, software license) or laws.

dd) The federal government has imposed restrictions on the exportation of encryption software or files containing encryption technology. Software containing restricted encryption technology shall not be transmitted outside the United States.

Inappropriate or Unlawful Materials

The following activities are strictly prohibited, with no exceptions:

ee) MS expressly forbids the storage, transmission, or viewing of any adult, offensive, intimidating, or hostile materials on any of the company's computing equipment or systems. MS forbids creating, sending, viewing, or receiving such materials in the workplace, in any form. If such material is introduced to your assigned equipment, you must eliminate such materials from their assigned equipment without forwarding them or making copies.

ff) Using the company's computing equipment to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in violation of State or Federal Law.

Connection of Unauthorized Equipment

The following activities are strictly prohibited, with no exceptions:

gg) Users are forbidden from connecting or using of any unauthorized equipment to the MS network.

hh) Unauthorized networking equipment (such as routers, switches, wireless access points, etc.) is prohibited from use on the network. All network infrastructure and wiring may not be modified or extended beyond their intended use.

ii) Unauthorized interference devices such as cell phone jammers designed or intended to interfere with MS systems or services is prohibited from use on the network or within the premises.

Transmission or Storage of Sensitive Data

The following activities are strictly prohibited, with no exceptions:

jj) Users are prohibited from storing or transmitting sensitive information on non-Company owned equipment. Sensitive data stored on company owned equipment is restricted to non-restricted confidential data. (*See Data Classification Policy*).

Monitored Use

The IT department shall implement, monitor, and evaluate the Company's network and technology resources for instructional and administrative purposes. Access to the system/network, including external networks, shall be made available to Contractors for business and administrative purposes only in accordance with administrative regulations and procedures. As a condition of use, all MS Contractors to include all authorized "Third-Party clients" waive any right to privacy in anything they create, store, send, disseminate, or receive via the company's information resource technology.

- The IT department has the authority and the right to monitor all aspects of its technology, including, but not limited to, monitoring computer and Internet activity of any system user.

- Electronic mail transmissions and other uses of electronic resources by Company's Contractors shall not be considered confidential and may be monitored at any time by designated IT staff to ensure appropriate use for instructional and administrative purposes.

- In the efforts to ensure compliance with this policy, Internet activities will be monitored by the IT department to ensure users are not accessing inappropriate (obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful) sites. The foregoing examples of inappropriate access are not intended to be all inclusive.

Enforcement

Any users found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. The IT department reserves the right, with the consent of the department head, to disconnect any host or network to prevent unauthorized activities.

Affiliate Network Partner Printed Name:

First Name: David Last Name: Collins

Signature:

Date: 2/5/2024