DATA PROTECTION POLICIES AND STANDARDS

Password Creation Guidelines

1. Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. The following guidelines provides best practices for creating secure passwords. The purpose of these guidelines is to provide best practices for the creation of strong passwords. These guidelines apply to all government employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

2. Policy

Strong passwords are long, the more the number of characters, stronger the password. There should be at least 14 characters in the password. In addition, passphrases, passwords made up of multiple words, should be used. Examples include “Let’s go out for a meal” or “interesting-cloudy-flowers-box”. Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak passwords can be guessed easily. Passwords can be categorised as poor or weak if they contain less than eight characters or contain personal information or easily recognisable patterns like a sequence of numbers of alphabets (aaabbb, 12345) or contain commonly used words like welcome, hello etc.

In addition, every work account should have a different, unique password. To maintain multiple passwords, ‘password manager’ software that is authorised and provided by the organisation should be used. Multi-factor authentication should be enabled whenever possible.

Password Protection Policy

1. Overview

Passwords are vital part of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of government resources. All staff members, including contractors and vendors with access to government systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords. The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any

system that resides at any government facility, has access to the government network, or stores any non-public government information.

2. Policy

2.1 Password Change

2.1.1 Passwords should be changed only when there is a reason to believe a password has been compromised.

2.1.2 Password cracking or guessing may be performed on a periodic or random basis by the Government Cyber Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

2.2 Password Protection

2.2.1 Passwords must not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as sensitive, Confidential government information.

2.2.2 Passwords must not be included into email messages, or other forms of electronic communication, nor revealed over the phone to anyone.

2.2.3 Passwords may be stored only in “password managers” authorised by the organisation.

2.2.4 The "Remember Password" feature of web browsers should not be used.

2.2.5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

2.3 Application Development

Application developers working for government must ensure that their programs contain the following security precautions:

2.3.1 Applications must support authentication of individual users.

2.3.2 Applications must not store passwords in clear text or in any easily reversible form.

2.3.3 Applications must not transmit passwords in clear text over the network.

2.3.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

2.4 Multi-Factor Authentication

2.4.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

Email Communication Policy

1. Overview

Electronic email is a commonly used communication and awareness method within the government organisation. Misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications. The purpose of this email policy is to ensure the proper use of government email system and make users aware of what government deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within government Network. It also covers appropriate use of any email sent from a government email address and applies to all employees, vendors, and agents operating on behalf of government.

2. Policy

2.1 All use of email must be consistent with government policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

2.2 Government email account should be used primarily for government administration-related purposes; personal communication is permitted on a limited basis, but non-government related commercial uses are prohibited.

2.3 All government data contained within an email message or an attachment must be secured according to the Data Protection Standard.

2.4 Email should be retained only if it qualifies as a government administration record. Email is a government administration record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

2.5 Email that is identified as a government administration record shall be retained according to government Record Retention Schedule.

2.6 The government email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any government employee should report the matter to their supervisor immediately.

2.7 Users are prohibited from automatically forwarding government email to a third party email system. Individual messages which are forwarded by the user must not contain government confidential or above information.

2.8 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct government administration activities, to create or memorialise any binding transactions, or to store or retain email on behalf of government. Such communications and transactions should be conducted through proper channels using government-approved documentation.

Data Breach Response Policy

1. Overview

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritisation of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicised and made easily available to all personnel whose duties involve data privacy and security protection.

Government Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how government's established culture of openness, trust and integrity should respond to such activity. Government Information Security is committed to protecting government's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

This policy mandates that any individual who suspects that a theft, breach or exposure of government Protected data or government Sensitive data has occurred must immediately provide a description of what occurred via e-mail, by calling number available on official web page, or through the use of the help desk reporting web page form. The e-mail address, phone number, and web page are monitored by the government's Information Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place. This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of government members.

2. Policy

As soon as a theft, data breach or exposure containing government Protected data or government Sensitive data is identified, the process of removing all access to that resource will begin.

The Executive Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Infrastructure
- IT Applications
- Finance (if applicable)
- Legal
- Communications
- Member Services (if Member data is affected)
- Human Resources
- The affected unit or department whose data may have been breached or exposed.
- Additional departments based on the data type involved.

The Executive Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyse the breach or exposure to determine the root cause.

Work with Forensic Investigators:

As provided by government cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/ external individuals and/or organisations impacted; and analyse the breach or exposure to determine the root cause.

Develop a communication plan:

This will involve working with government communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the government community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any government Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.

- Information Security Administrator is that member of the government community, designated by the Executive Director or the Director, Information

Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.

- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.
- Any government personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

Acceptable Use Policy

1. Overview

This policy is designed for protecting government's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

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 government. These systems are to be used only for serving the interests of the government.

The purpose of this policy is to outline the acceptable use of computer equipment at government offices. These rules are in place to protect the employees and government. Inappropriate use exposes government to risks including virus attacks, compromise of network systems and services, and legal issues.

This policy applies to the use of information, electronic and computing devices, and network resources to conduct government administration activities or interact with internal networks and business systems, whether owned or leased by government, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at government and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with government policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at government, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by government.

2. Policy

2.1 General Use and Ownership

2.1.1 Government proprietary information stored on electronic and computing devices whether owned or leased by government, the employee or a third party, remains the sole property of government. This information must be protected in accordance with the Data Protection Standard through legal or technical means.

2.1.2 Employees have a responsibility to promptly report the theft, loss or unauthorised disclosure of government proprietary information.

2.1.3 Employees may access, use or share government proprietary information only to the extent it is authorised and necessary to fulfil their assigned job duties.

2.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

2.1.5 For security and network maintenance purposes, authorised individuals within government may monitor equipment, systems and network traffic at any time, per government's Audit Policy.

2.1.6 Government reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.2 Security and Proprietary Information

2.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

2.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

2.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Employees must lock the screen or log off when the device is unattended.

2.2.4 Postings by employees from a government email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of government, unless posting is in the course of business duties.

2.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

2.3 Blogging and Social Media

2.3.1 Blogging by employees, whether using government's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of government's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate government's policy, is not detrimental to government's best interests, and does not interfere with an employee's regular work duties. Blogging from government's systems is also subject to monitoring.

2.3.2 Government's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any government confidential or proprietary information, trade secrets or any other material covered by government's Confidential Information policy when engaged in blogging.

2.3.3 Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of government and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by government's Non-Discrimination and Anti-Harassment policy.

2.3.4 Employees may also not attribute personal statements, opinions or beliefs to government when engaged in blogging. Employees assume any and all risk associated with blogging.

2.3.5 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, government's trademarks, logos and any other government intellectual property may also not be used in connection with any blogging activity.

Clean Desk Policy

1. Overview

A clean desk policy can be an important tool to ensure that all sensitive/ confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilise when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

The purpose for this policy is to establish the minimum requirements for maintaining a “clean desk” – where sensitive/critical information about government employees, government’s intellectual property, customers and vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

This policy applies to all government employees and affiliates.

2. Policy

2.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

2.2 Computer workstations must be locked when workspace is unoccupied.

2.3 Computer workstations must be shut completely down at the end of the work day.

2.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

2.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

2.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

2.7 Laptops must be either locked with a locking cable or locked away in a drawer.

2.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

2.9 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

2.10 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

2.11 Whiteboards containing Restricted and/or Sensitive information should be erased.

2.12 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.

All printers and fax machines should be cleared of papers as soon as they are printed. This helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Bluetooth Usage Policy

1. Overview

Insecure Bluetooth connections can introduce a number of potential serious security issues. Hence, there is a need for a minimum standard for connecting Bluetooth enabled devices.

The purpose of this policy is to provide a minimum baseline standard for connecting Bluetooth enabled devices to the government network or government-owned devices. The intent of the minimum standard is to ensure sufficient protection of Personally Identifiable Information (PII) and confidential government data.

This policy applies to any Bluetooth enabled device that is connected to government network or owned devices.

2. Policy

2.1 Pins and Pairing

When pairing the Bluetooth unit to Bluetooth enabled equipment (i.e. phone, laptop, etc.), employees must ensure that they are not in a public area where their PIN can be compromised.

If the Bluetooth enabled equipment asks to enter the pin even after the initial pairing, employees must refuse the pairing request and report it to government IT officials, through Help Desk, immediately.

2.2 Device Security Settings

• All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between the Bluetooth Device and its paired equipment. Employees must:

• Use a minimum PIN length of 8. A longer PIN provides more security.

• Switch the Bluetooth device to use the hidden mode (non-discoverable)

• Only activate Bluetooth only when it is needed.

• Ensure device firmware is up-to-date.

2.4 Security Audits

The government IT Team may perform random audits to ensure compliance with this policy. In the process of performing such audits, government IT Team members shall not eavesdrop on any phone conversation.

2.5 User Responsibilities

• Bluetooth mode must be turned off when not in use.

• PII and/or government Confidential or Sensitive data must not be transmitted or stored on Bluetooth enabled devices.

• Bluetooth users must only access government information systems using approved Bluetooth device hardware, software, solutions, and connections.

• Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorised for deployment.

• Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to government IT Department.

Remote Access Policy

1. Overview

Remote access to government network is essential to maintain productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than government's network. While these remote networks are beyond the control of Hypergolic Reactions, LLC policy, employees must try to mitigate these external risks to the best of their ability.

The purpose of this policy is to define rules and requirements for connecting to government's network from any host. These rules and requirements are designed to minimise the potential exposure to government from damages which may result from unauthorised use of government resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical government internal systems, and fines or other financial liabilities incurred as a result of those losses.

This policy applies to all government employees, contractors, vendors and agents with a government-owned or personally-owned computer or workstation used to connect to the government network. This policy applies to remote access connections used to do work on behalf of government, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to government networks.

2. Policy

It is the responsibility of government employees, contractors, vendors and agents with remote access privileges to government's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to government.

General access to the Internet for recreational use through the government network is strictly limited to government employees, contractors, vendors and agents. When accessing the government network from a personal computer, authorised users are responsible for preventing access to any government computer resources or data by non-authorised users. Performance of illegal activities through the government network by any user (authorised or otherwise) is prohibited. The authorised user bears responsibility for and consequences of misuse of the authorised user's access.

2.1 Requirements

2.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases.

2.1.2 Authorised users shall protect their login and password, even from family members.

2.1.3 While using a government-owned computer to remotely connect to government's corporate network, authorised users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an authorised user or third party.

2.1.4 Use of external resources to conduct government business must be approved in advance by government IT Department and the appropriate business unit manager.

2.1.5 All hosts that are connected to government internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.

2.1.6 Personal equipment used to connect to government's networks must meet the requirements of government-owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to government Networks.

Wireless Communication Policy

1. Overview

Insecure wireless configuration can provide an easy open door for malicious threat actors.

The purpose of this policy is to secure and protect the information assets owned by government. Government provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives.

Government grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to government network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a government network.

All employees, contractors, consultants, temporary and other workers at government, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of government must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a government network or reside on a government site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

2. Policy

2.1 General Requirements

All wireless infrastructure devices that reside at a government site and connect to a government network, or provide access to information classified as government Confidential, or above must:

• Abide by the standards specified in the Wireless Communication Standard.

• Be installed, supported, and maintained by an approved support team.

• Use government approved authentication protocols and infrastructure.

• Use government approved encryption protocols.

• Maintain a hardware address (MAC address) that can be registered and tracked.

• Not interfere with wireless access deployments maintained by other support organisations.

2.2 Lab and Isolated Wireless Device Requirements

Lab and isolated wireless devices that do not provide general network connectivity to the government network must be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the Lab Security Policy. They should not interfere with wireless access deployments maintained by other support organisations.

2.3 Home Wireless Device Requirements

2.3.1 Wireless infrastructure devices that provide direct access to the government corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.

2.3.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the government corporate network. Access to the government corporate network through this device must use standard remote access authentication.

Equipment Disposal Policy

1. Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of government data, some of which is considered sensitive. In order to protect government's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

The purpose of this policy is to define the guidelines for the disposal of technology equipment and components owned by government.

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within government including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials.

All government employees and affiliates must comply with this policy.

2. Policy

2.1 Technology Equipment Disposal

2.1.1 When Technology assets have reached the end of their useful life they should be sent to the Equipment Disposal Team office for proper disposal.

2.1.2 The Equipment Disposal Team will securely erase all storage mediums in accordance with current industry best practices.

2.1.3 All data including, all files and licensed software shall be removed from equipment using disk sanitising software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defence standards.

2.1.4 No computer or technology equipment may be sold to any individual other than through the processes identified in this policy.

2.1.5 No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around government. These can be used to dispose of equipment. The Equipment Disposal Team will properly remove all data prior to final disposal.

2.1.6 All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

2.1.7 Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

2.1.8 The Equipment Disposal Team will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.

2.1.9 Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

Anti-Virus Guidelines

Recommended processes to prevent virus problems:

• Always run the Corporate standard, download and install anti-virus software updates as they become available.

• NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

• Delete spam, chain, and other junk email without forwarding, in keeping with government's Acceptable Use Policy.

• Never download files from unknown or suspicious sources.

• Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

• Always scan a floppy diskette from an unknown source for viruses before using it.

• Back-up critical data and system configurations on a regular basis and store the data in a safe place.

• If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

• New viruses are discovered almost every day. Periodically check the Lab Anti-Virus Policy and this Recommended Processes list for updates.

Internet usage Policy

1. Overview

Internet connectivity presents the government with new risks that must be addressed to safeguard vital information assets.

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

Access to the Internet will be provided to users to support government operations and only on an as-needed basis to perform their jobs and professional roles.

The purpose of this policy is to define the appropriate uses of the Internet by government employees and affiliates.

The Internet usage Policy applies to all Internet users (individuals working for the government, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The government's Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

Internet Services Allowed:

Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

• E-mail: Send/receive E-mail messages to/from the Internet (with or without document attachments).

• Navigation: WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated government public web servers only.

• File Transfer Protocol (FTP): Send data/files and receive in-bound data/files, as necessary for business purposes.

• Telnet: Standard Internet protocol for terminal emulation. User Strong Authentication required for Internet initiated contacts into the company.

Management reserves the right to add or delete services as business needs change or conditions warrant.

All other services will be considered unauthorised access to/from the Internet and will not be allowed.

Request & Approval Procedures:

Internet access will be provided to users to support government operations and only as needed to perform their jobs.

Request for Internet Access:

As part of the Internet access request process, the employee is required to read both this Internet usage Policy and the associated Internet/Intranet Security Policy. The user must then sign the statements (located on the last page of each document) that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action up to and including termination.

Policy awareness and acknowledgment, by signing the acknowledgment form, is required before access will be granted.

Approval:

Internet access is requested by the user or user's manager submitting an IT Access Request form to the IT department along with an attached copy of a signed Internet usage Coverage Acknowledgment Form.

Removal of privileges:

Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In

response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

2. Policy

2.1 Resource Usage

Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another business unit or changes job functions within the government, a new Internet access request must be submitted within 5 days.

User Internet access requirements will be reviewed periodically by government's departments to ensure that continuing needs exist.

2.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes;
- IT technical support downloading software upgrades and patches;
- Review of possible vendor web sites for product information;
- Reference regulatory or technical information.
- Research

2.3 Personal Usage

Using government-owned computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the government network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The government is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property

2.4 Software License

The government strongly supports strict adherence to software vendors' license agreements. When at work, or when government's computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal Department before any copying is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

Using government-owned computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

2.5 Review of Public Information

All publicly-writeable directories on Internet-connected computers will be reviewed and cleared each evening. This process is necessary to prevent the anonymous exchange of information inconsistent with government operations. Examples of unauthorised public information include pirated information, passwords, credit card numbers, and pornography.

2.6 Expectation of Privacy

2.6.1 Monitoring

Users should consider their Internet activities as periodically monitored and limit their activities accordingly. Management reserves the right to examine E-mail, personal file directories, web access, and other information stored on government-owned computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

2.6.2 E-mail Confidentiality

Users should be aware that clear text E-mail is not a confidential means of communication. The government cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

2.7 Periodic Reviews

2.7.1 Usage Compliance Reviews

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

2.7.2 Policy Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit company information needs.

Virtual Private Network (VPN) Policy

1. Overview

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the government network.

This policy applies to all government employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilising VPNs to access the government network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

2. Policy

Approved government employees and authorised third parties (customers, vendors, etc.) may utilise the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorised users are not allowed access to government internal networks.

2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

3. When actively connected to the government network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

4. Dual (split) tunnelling is NOT permitted; only one network connection is allowed.

5. VPN gateways will be set up and managed by government network operational groups.

6. All computers connected to government internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.

7. VPN users will be automatically disconnected from government's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

8. The VPN concentrator is limited to an absolute connection time of 24 hours.

9. Users of computers that are not government-owned equipment must configure the equipment to comply with government's VPN and Network policies.

10. Only government IT-approved VPN clients may be used.

11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of government's network, and as such are subject to the same rules and regulations that apply to government-owned equipment, i.e., their machines must be configured to comply with government's IT Security Policies.

Mobile Devices Policy

1. Overview

This policy describes Information Security's requirements for employees of government that work outside of an office setting.

This policy applies to any mobile device, or endpoint computer issued by government or used for government business which contains stored data owned by government.

2. Policy

All employees shall assist in protecting devices issued by government or storing government data. Mobile devices are defined to include desktop systems in a telework environment, laptops, PDAs, and cell phones.

Users are expressly forbidden from storing government data on devices that are not issued by government, such as storing government email on a personal cell phone or PDA.

2.1 Anti-Virus and Endpoint Security Software

Government will issue computers with Anti-virus and Endpoint security installed. Employees are to notify the security department immediately if they see error messages for these products. Employees shall run on online malware scanner at

least once a month for a “second opinion”, see MS Endpoint Privacy & Security Guidelines for recommended scanners.

2.2 Browser Add-ons

In general, government does not recommend using Browser Add-ons, however it is not forbidden to use these tools if they enhance productivity. After installing a Browser Add-on, employees shall run a browser testing tool.

IMPLEMENTATION PLANS FOR POLICIES

Role of cyber security experts:

For the implementation of the policies the government should appoint a panel of cyber security experts, who will ensure all security protocols are followed. The implementation of the policies and cyber code of conduct will be the main responsibility of panel. The government should appoint the director who will control the team and guide them as required. The other government departments will have communication with the director.

Any request made by employee should be handled by appointed team and should respond in compliance with the request made through e-mail communication only.

Secure conditions for cyber security can be established by creating a platform of cooperation between government staff and cyber security experts. An inter-departmental working group can be created to deal with large scale cyber attacks . This ensures fast response in a situation of potential threat.

A procedure must be defined for institutional management of cyber security in case of emergency. Cyber security experts should establish central access points to protect critical infrastructure elements.

The panel can also can formulate a risk assessment plan to understand risk level at any point. If a potential risk is detected, they can propose security measures necessary to mitigate or minimise the risk. They can suggest new security measures or protocols that will minimise such risks in future.

To ensure all security measures are in place, the panel members can conduct penetration tests of government’s information systems including critical infrastructure elements.

The cyber security experts can evaluate current status of awareness among the staff members by conducting awareness trainings and tests. Based on the results, they can innovate and improvise the training program in order to make all staff members aware of the potential threats posed by cyber attacks. They can expand the content of existing training to include specific new areas. An effective online

system for reporting and responding to security incidents can be useful when dealing with any potential breach. The cyber security team can also approach concerned government officials for support in research activities in the field of cyber security in order to stay up to date with all the latest developments.

Policy Compliance:

Compliance Measurement

The cyber security experts appointed by government will ensure compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and regular feedbacks.

Exceptions:

Any exception to the policy must be approved by the government IT team in advance.

Non-Compliance:

An employee found to have violated a policy may be subject to disciplinary action, up to and including termination of employment.

Schedule for Audit:

The appointed panel of cyber security experts will perform audit for various levels and generated report will be submitted to concerned department of government. Any non-compliance by government staff observed during audit should be noted and appropriate action must be taken to ensure it does not expose any confidential information.

Actions:

As per the audit reports generated the appointed panel should recommend any change in existing policy if required.

As an output of your earlier analysis, panel should have a list of risks, organised by impact. Depending on the government's Data Privacy requirements and risk level, a set of controls is necessary in order to either mitigate, avoid, transfer, or accept the risks. This will include both technical and non-technical controls.

A robust and comprehensive cyber security policy is a fundamental part of government's data protection strategy. To make these policies more effective, they should me made with input from all the government departments and should take into account the needs for all of the government staff members. Although basic structure of the policies remains constant, taking time to make changes in the policy according to specific needs and constantly updating the policies to make sure all new threats can be dealt with effectively ensures protection of government's assets and confidential information.

References:

https://www.sans.org/security-resources/policies/retired#anti-virus-guidelines

https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html

https://www.housing.gov.ie/sites/default/files/publications/files/data-protection-policy.pdf

https://doit.missouri.edu/about/policies-procedures/data-center-policies-procedures/

https://www.foundation.cpp.edu/content/f/d/mis/DCA-policies-procedures.pdf

https://www.mcpressonline.com/analytics-cognitive/business-intelligence/setting-data-policies-standards-and-processes

https://resources.infosecinstitute.com/how-to-implement-a-data-privacy-strategy-10-steps/#gref

https://www.sans.org/security-resources/policies

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ActionPlanfortheImplementationoftheCyberSecurityConceptoftheSlovakRepublicfor20152020_3_.pdf