Annexure – 'A'

1. Account Policies
    a. Password Policy
        i. Ensure 'Enforce password history' is set to '24 or more password(s)'
        ii. Ensure 'Maximum password age' is set to '90 days, but not 0'
        iii. Ensure 'Minimum password age' is set to '1 day'
        iv. Ensure 'Minimum password length' is set to '12 or more character(s)'
        v. Ensure 'Password must meet complexity requirements' is set to 'Enabled'
        vi. Ensure 'Store passwords using reversible encryption' is set to 'Disabled'
    b. Account Lockout Policy
        i. Ensure 'Account lockout duration' is set to '15 or more minute(s)'
        ii. Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'
        iii. Ensure 'Allow Administrator account lockout' is set to 'Enabled' (Manual)

2. Local Policies
    a. User Rights Assignment
        i. Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'
        ii. Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'
        iii. Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'
        iv. Ensure 'Allow log on locally' is set to 'Administrators, Users'
        v. Ensure 'Back up files and directories' is set to 'Administrators'
        vi. Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'
        vii. Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users'
3. Security Options
    a. Accounts
        i. Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'
        ii. Ensure 'Accounts: Guest account status' is set to 'Disabled'

iii. Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'
iv. Configure 'Accounts: Rename administrator account'
v. Configure 'Accounts: Rename guest account'

b. Interactive logon
   i. Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'
   ii. Ensure 'Interactive logon: Don't display last signed in' is set to 'Enabled'
   iii. Ensure 'Interactive logon: Machine account lockout threshold' is set to '10 or fewer invalid logon attempts, but not 0'
   iv. Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'
   v. Configure 'Interactive logon: Message text for users attempting to log on'
   vi. Configure 'Interactive logon: Message title for users attempting to log on'
   vii. Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'

c. Microsoft network server
   i. Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'
   ii. Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'
   iii. Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'
   iv. Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'
   v. Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'
   vi. Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'
   vii. Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'

d. Network security

i. Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'
ii. Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'
iii. Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher
iv. Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'
v. Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

4. System settings
   a. User Account Control
      i. Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'
      ii. Ensure 'User Account Control: Behaviour of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher
      iii. Ensure 'User Account Control: Behaviour of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'
      iv. Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'
      v. Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'
      vi. Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'

   b. System Services
      i. Ensure 'Bluetooth Audio Gateway Service (BTAGService)' is set to 'Disabled'
      ii. Ensure 'Bluetooth Support Service (bthserv)' is set to 'Disabled'
      iii. Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'
      iv. Ensure 'Geolocation Service (lfsvc)' is set to 'Disabled'
      v. Ensure 'Internet Connection Sharing (ICS) (SharedAccess)' is set to 'Disabled'

vi. Ensure 'Remote Desktop Configuration (SessionEnv)' is set to 'Disabled'
vii. Ensure 'Remote Desktop Services (TermService)' is set to 'Disabled'
viii. Ensure 'Remote Desktop Services UserMode Port Redirector (UmRdpService)' is set to 'Disabled'
ix. Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled'
x. Ensure 'Remote Registry (RemoteRegistry)' is set to 'Disabled'
xi. Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled'
xii. Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Disabled' or 'Not Installed'
xiii. Ensure 'SNMP Service (SNMP)' is set to 'Disabled' or 'Not Installed'
xiv. Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled'
xv. Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed'
xvi. Ensure 'Windows Error Reporting Service (WerSvc)' is set to 'Disabled'
xvii. Ensure 'Windows Event Collector (Wecsvc)' is set to 'Disabled'
xviii. Ensure 'Windows Media Player Network Sharing Service (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed'
xix. Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled'
xx. Ensure 'Windows PushToInstall Service (PushToInstall)' is set to 'Disabled'
xxi. Ensure 'Windows Remote Management (WS Management) (WinRM)' is set to 'Disabled'
xxii. Ensure 'World Wide Web Publishing Service (W3SVC)' is set to 'Disabled' or 'Not Installed'
xxiii. Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled'
xxiv. Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled'
xxv. Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled'
xxvi. Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled'

5. Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)

a. Private Profile
    i. Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'
    ii. Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)
    iii. Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'
    iv. Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'
    v. Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (
    vi. Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'
    vii. Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'
    viii. Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'
b. Public Profile
    i. Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)
    ii. Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'
    iii. Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'
    iv. Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'
    v. Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'
    vi. Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'
    vii. Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log'
    viii. Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'
    ix. Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'
    x. Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'

6. Advanced Audit Policy Configuration
    a. Account Logon
        i. Ensure 'Audit Credential Validation' is set to 'Success and Failure'

ii. Ensure 'Audit Application Group Management' is set to 'Success and Failure'
iii. Ensure 'Audit Security Group Management' is set to include 'Success'
iv. Ensure 'Audit User Account Management' is set to 'Success and Failure'
v. Ensure 'Audit PNP Activity' is set to include
vi. Ensure 'Audit Process Creation' is set to include 'Success'
vii. Ensure 'Audit Account Lockout' is set to include 'Failure'
viii. Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'
ix. Ensure 'Audit File Share' is set to 'Success and Failure'
x. Ensure 'Audit Removable Storage' is set to 'Success and Failure'
xi. Ensure 'Audit Audit Policy Change' is set to include 'Success'
xii. Ensure 'Audit Other Policy Change Events' is set to include 'Failure'
xiii. Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'
xiv. Ensure 'Audit System Integrity' is set to 'Success and Failure'
xv. Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'
xvi. Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'
xvii. Ensure 'Configure SMB v1 server' is set to 'Disabled'

b. AutoPlay Policies
i. Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'
ii. Ensure 'Set the default behaviour for AutoRun' is set to 'Enabled: Do not execute any autorun commands'
iii. Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'

7. Microsoft Defender Application Guard (formerly Windows Defender Application Guard)

a. Ensure 'Allow auditing events in Microsoft Defender Application Guard' is set to 'Enabled'

b. Ensure 'Allow camera and microphone access in Microsoft Defender Application Guard' is set to 'Disabled'

c. Ensure 'Allow data persistence for Microsoft Defender Application Guard' is set to 'Disabled'

d. Ensure 'Allow files to download and save to the host operating system from Microsoft Defender Application Guard' is set to 'Disabled'

e. Ensure 'Configure Microsoft Defender Application Guard clipboard settings: Clipboard behaviour setting' is set to 'Enabled: Enable clipboard operation from an isolated session to the host'

Annexure – 'B'

1. Filesystem
    a. Configure Filesystem Kernel Modules
        i. Ensure cramfs kernel module is not available
        ii. Ensure freevxfs kernel module is not available
        iii. Ensure hfs kernel module is not available
        iv. Ensure hfsplus kernel module is not available
        v. Ensure jffs2 kernel module is not available
        vi. Ensure overlayfs kernel module is not available
        vii. Ensure squashfs kernel module is not available
        viii. Ensure udf kernel module is not available
        ix. Ensure usb-storage kernel module is not available
        x. Ensure unused filesystems kernel modules are not available

    b. Configure Filesystem Partitions
        i. Configure /tmp 1.1.2.1.1 Ensure /tmp is a separate partition
        ii. Ensure nodev option set on /tmp partition
        iii. Ensure nosuid option set on /tmp partition
        iv. Ensure noexec option set on /tmp partition

    c. Configure /dev/shm
        i. Ensure /dev/shm is a separate partition
        ii. Ensure nodev option set on /dev/shm partition
        iii. Ensure nosuid option set on /dev/shm partition
        iv. Ensure noexec option set on /dev/shm partition

    d. Configure /home
        i. Ensure separate partition exists for /home
        ii. Ensure nodev option set on /home partition
        iii. Ensure nosuid option set on /home partition

    e. Configure /var
        i. Ensure separate partition exists for /var
        ii. Ensure nodev option set on /var partition
        iii. Ensure nosuid option set on /var partition

    f. Configure /var/tmp
        i. Ensure separate partition exists for /var/tmp
        ii. Ensure nodev option set on /var/tmp partition
        iii. Ensure nosuid option set on /var/tmp partition
        iv. Ensure noexec option set on /var/tmp partition

g. Configure /var/log
    i. Ensure separate partition exists for /var/log
    ii. Ensure nodev option set on /var/log partition
    iii. Ensure nosuid option set on /var/log partition
    iv. Ensure noexec option set on /var/log partition
    v. Configure /var/log/audit

h. Ensure separate partition exists for /var/log/audit
    i. Ensure nodev option set on /var/log/audit partition
    ii. Ensure nosuid option set on /var/log/audit partition
    iii. Ensure noexec option set on /var/log/audit partition

2. Package Management
   a. Configure Bootloader
       i. Ensure bootloader password is set
       ii. Ensure access to bootloader config is configured

   b. Configure Additional Process Hardening
       i. Ensure address space layout randomization is enabled
       ii. Ensure ptrace_scope is restricted
       iii. Ensure core dumps are restricted
       iv. Ensure prelink is not installed
       v. Ensure Automatic Error Reporting is not enabled

   c. Configure Command Line Warning Banners
       i. Ensure local login warning banner is configured properly
       ii. Ensure remote login warning banner is configured properly
       iii. Ensure access to /etc/motd is configured
       iv. Ensure access to /etc/issue is configured
       v. Ensure access to /etc/issue.net is configured

3. Services
   a. Configure Server Services
       i. Ensure autofs services are not in use
       ii. Ensure avahi daemon services are not in use
       iii. Ensure dhcp server services are not in use
       iv. Ensure dns server services are not in use
       v. Ensure dnsmasq services are not in use
       vi. Ensure ftp server services are not in use
       vii. Ensure ldap server services are not in use
       viii. Ensure message access server services are not in use
       ix. Ensure network file system services are not in use

x. Ensure nis server services are not in use
xi. Ensure print server services are not in use
xii. Ensure rpcbind services are not in use
xiii. Ensure rsync services are not in use
xiv. Ensure samba file server services are not in use
xv. Ensure snmp services are not in use
xvi. Ensure tftp server services are not in use
xvii. Ensure web proxy server services are not in use
xviii. Ensure web server services are not in use
xix. Ensure xinetd services are not in use
xx. Ensure X window server services are not in use
xxi. Ensure mail transfer agent is configured for local-only mode
xxii. Ensure only approved services are listening on a network interface

b. Configure Client Services
   i. Ensure NIS Client is not installed
   ii. Ensure rsh client is not installed
   iii. Ensure talk client is not installed
   iv. Ensure telnet client is not installed
   v. Ensure ldap client is not installed
   vi. Ensure ftp client is not installed
   vii. Configure Time Synchronization

c. Ensure time synchronization is in use
   i. Ensure a single time synchronization daemon is in use

d. Configure systemd-timesyncd
   i. Ensure systemd-timesyncd configured with authorized timeserver
   ii. Ensure systemd-timesyncd is enabled and running

e. Configure chrony
   i. Ensure chrony is configured with authorized timeserver
   ii. 2.3.3.2 Ensure chrony is running as user _chrony
   iii. 2.3.3.3 Ensure chrony is enabled and running

f. Job Schedulers
   i. Ensure cron daemon is enabled and active
   ii. Ensure permissions on /etc/crontab are configured
   iii. Ensure permissions on /etc/cron.hourly are configured
   iv. Ensure permissions on /etc/cron.daily are configured
   v. Ensure permissions on /etc/cron.weekly are configured

vi. Ensure permissions on /etc/cron.monthly are configured
vii. Ensure permissions on /etc/cron.d are configured
viii. Ensure crontab is restricted to authorized users

4. Network
   a. Configure Network Devices
      i. Ensure IPv6 status is identified
      ii. Ensure wireless interfaces are disabled
      iii. Ensure bluetooth services are not in use

   b. Configure Network Kernel Modules
      i. Ensure dccp kernel module is not available
      ii. Ensure tipc kernel module is not available
      iii. Ensure rds kernel module is not available
      iv. Ensure sctp kernel module is not available

   c. Configure Network Kernel Parameters
      i. Ensure ip forwarding is disabled
      ii. Ensure packet redirect sending is disabled
      iii. Ensure bogus icmp responses are ignored
      iv. Ensure broadcast icmp requests are ignored
      v. Ensure icmp redirects are not accepted
      xi. Ensure secure icmp redirects are not accepted
      xii. Ensure reverse path filtering is enabled
      xiii. Ensure source routed packets are not accepted
      xiv. Ensure suspicious packets are logged
      xv. Ensure tcp syn cookies is enabled
      xvi. Ensure ipv6 router advertisements are not accepted

5. Host Based Firewall
   a. Configure a single firewall utility
      i. Ensure ufw is installed
      ii. Ensure iptables-persistent is not installed with ufw
      iii. Ensure ufw service is enabled
      iv. Ensure ufw loopback traffic is configured
      v. Ensure ufw outbound connections are configured (Manual)
      vi. Ensure ufw firewall rules exist for all open ports
      vii. Ensure ufw default deny firewall policy
      viii. Ensure ufw is not in use with iptables

6. Access Control
   a. Configure SSH Server

i. Ensure permissions on /etc/ssh/sshd_config are configured
ii. Ensure permissions on SSH private host key files are configured
iii. Ensure permissions on SSH public host key files are configured
iv. Ensure sshd access is configured
v. Ensure sshd Banner is configured
vi. Ensure sshd Ciphers are configured
vii. Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured
viii. Ensure sshd DisableForwarding is enabled
ix. Ensure sshd GSSAPIAuthentication is disabled
x. Ensure sshd HostbasedAuthentication is disabled
xi. Ensure sshd IgnoreRhosts is enabled
xii. Ensure sshd KexAlgorithms is configured
xiii. Ensure sshd LoginGraceTime is configured
xiv. Ensure sshd LogLevel is configured
xv. Ensure sshd MACs are configured
xvi. Ensure sshd MaxAuthTries is configured
xvii. Ensure sshd MaxSessions is configured
xviii. Ensure sshd MaxStartups is configured
xix. Ensure sshd PermitEmptyPasswords is disabled
xx. Ensure sshd PermitRootLogin is disabled
xxi. Ensure sshd PermitUserEnvironment is disabled
xxii. Ensure sshd UsePAM is enabled

b. Configure privilege escalation
i. Ensure sudo is installed
ii. Ensure sudo commands use pty
iii. Ensure sudo log file exists
iv. Ensure users must provide password for privilege escalation
v. Ensure re-authentication for privilege escalation is not disabled globally
vi. Ensure sudo authentication timeout is configured correctly
vii. Ensure access to the su command is restricted

c. Pluggable Authentication Modules
i. Configure PAM software packages
1. Ensure latest version of pam is installed
2. Ensure libpam-modules is installed
3. Ensure libpam-pwquality is installed

ii. Configure pam-auth-update profiles
    1. Ensure pam_unix module is enabled
    2. pam_faillock module is enabled
    3. Ensure pam_pwquality module is enabled
    4. Ensure pam_pwhistory module is enabled

iii. Configure pam_faillock module
    1. Ensure password failed attempts lockout is configured
    2. password unlock time is
    3. Ensure password failed attempts lockout includes root account

iv. Configure pam_pwquality module
    1. Ensure password number of changed characters is configured
    2. Ensure minimum password length is configured
    3. Ensure password same consecutive characters is configured
    4. Ensure password maximum sequential characters is configured
    5. Ensure password dictionary check is enabled
    6. Ensure password quality checking is enforced
    7. Ensure password quality is enforced for the root user

v. Configure pam_pwhistory module
    1. Ensure password history remember is configured
    2. Ensure password history is enforced for the root user
    3. Ensure pam_pwhistory includes use_authtok

7. User Accounts and Environment
    a. Configure shadow password suite parameters
        i. Ensure password expiration is configured
        ii. Ensure minimum password days is configured (Manual)
        iii. Ensure password expiration warning days is configured
        iv. Ensure strong password hashing algorithm is configured
        v. Ensure inactive password lock is configured
        vi. Ensure all users last password change date is in the past
        vii. Configure root and system accounts and environment
        5.4.2.1 Ensure root is the only UID 0 account
        viii. Ensure root is the only GID 0 account
        ix. Ensure group root is the only GID 0 group

x. Ensure root account access is controlled
xi. Ensure root path integrity
xii. Ensure root user umask is configured
xiii. Ensure system accounts do not have a valid login shell
xiv. Ensure accounts without a valid login shell are locked

b. Configure user default environment
i. Ensure nologin is not listed in /etc/shells
ii. Ensure default user shell timeout is configured
iii. Ensure default user umask is configured

8. Logging and Auditing
a. System Logging
i. Configure systemd-journald service
1. Ensure journald service is enabled and active
2. Ensure journald log file access is configured
3. Ensure journald log file rotation is configured
4. Ensure only one logging system is in use

ii. Configure rsyslog
1. Ensure rsyslog is installed
2. Ensure rsyslog service is enabled and active
3. Ensure journald is configured to send logs to rsyslog
4. Ensure rsyslog log file creation mode is configured
5. Ensure rsyslog logging is configured
6. Ensure rsyslog is configured to send logs to a remote log host
7. Ensure rsyslog is not configured to receive logs from a remote client
8. Ensure logrotate is configured

iii. Configure Logfiles
1. Ensure access to all logfiles has been configured

b. System Auditing
i. Configure auditd Service
1. Ensure auditd packages are installed
2. Ensure auditd service is enabled and active
3. Ensure auditing for processes that start prior to auditd is enabled
4. Ensure audit_backlog_limit is sufficient

c. Configure Data Retention

i. Ensure audit log storage size is configured
ii. Ensure audit logs are not automatically deleted
iii. Ensure system is disabled when audit logs are full
iv. Ensure system warns when audit logs are low on space

d. Configure auditd Rules
i. Ensure changes to system administration scope (sudoers) is collected
ii. Ensure actions as another user are always logged
iii. Ensure events that modify the sudo log file are collected
iv. Ensure events that modify date and time information are collected
v. Ensure events that modify the system's network environment are collected
vi. Ensure use of privileged commands are collected
vii. Ensure unsuccessful file access attempts are collected
viii. Ensure events that modify user/group information are collected
ix. Ensure discretionary access control permission modification events are collected
x. Ensure successful file system mounts are collected
xi. Ensure session initiation information is collected
xii. Ensure login and logout events are collected
xiii. Ensure file deletion events by users are collected
xiv. Ensure events that modify the system's Mandatory Access Controls are collected
xv. Ensure successful and unsuccessful attempts to use the chcon command are collected
xvi. Ensure successful and unsuccessful attempts to use the setfacl command are collected
xvii. Ensure successful and unsuccessful attempts to use the chacl command are collected
xviii. Ensure successful and unsuccessful attempts to use the usermod command are collected
xix. Ensure kernel module loading unloading and modification is collected
xx. Ensure the audit configuration is immutable
xxi. Ensure the running and on disk configuration is the same

e. Configure auditd File Access
i. Ensure audit log files mode is configured
ii. Ensure audit log files owner is configured
iii. Ensure audit log files group owner is configured
iv. Ensure the audit log file directory mode is configured
v. Ensure audit configuration files mode is configured
vi. Ensure audit configuration files owner is configured

vii. Ensure audit configuration files group owner is configured
viii. Ensure audit tools mode is configured
ix. Ensure audit tools owner is configured
x. Ensure audit tools group owner is configured

f. Configure Integrity Checking
i. Ensure AIDE is installed
ii. Ensure filesystem integrity is regularly checked
iii. Ensure cryptographic mechanisms are used to protect the integrity of audit tools

9. System Maintenance
a. System File Permissions
i. Ensure permissions on /etc/passwd are configured
ii. Ensure permissions on /etc/passwd- are configured
iii. Ensure permissions on /etc/group are configured
iv. Ensure permissions on /etc/group- are configured
v. Ensure permissions on /etc/shadow are configured
vi. Ensure permissions on /etc/shadow- are configured
vii. Ensure permissions on /etc/gshadow are configured
viii. Ensure permissions on /etc/gshadow- are configured
ix. Ensure permissions on /etc/shells are configured
x. Ensure permissions on /etc/security/opasswd are configured
xi. Ensure world writable files and directories are secured
xii. Ensure no files or directories without an owner and a group exist
xiii. Ensure SUID and SGID files are reviewed (Manual)
xiv. Local User and Group Settings 7.2.1 Ensure accounts in /etc/passwd use shadowed passwords
xv. Ensure /etc/shadow password fields are not empty
xvi. Ensure all groups in /etc/passwd exist in /etc/group
xvii. Ensure shadow group is empty
xviii. Ensure no duplicate UIDs exist Set Correctly Yes No
xix. Ensure no duplicate GIDs exist
xx. Ensure no duplicate user names exist
xxi. Ensure no duplicate group names exist
xxii. Ensure local interactive user home directories are configured
xxiii. Ensure local interactive user dot files access is configured

Organization: National Technical Research Organisation
Category: Software
Theme: Cyber Security
Video Link: N/A; **Dataset Link:** N/A