WTD Printing Products Security Requirements Appendix G

1 ACCESS AGREEMENTS *(MFD & MPS)*

The Contractor must have access agreements to the MPS where:

a. prior to being granted access to the MPS or Data, Administrators must sign an access agreement that lists the formal sanctions process for failing to comply with the terms and conditions of the access agreement, and

b. the Contractor must review and update access agreements to the MPS or Data on an annual basis.

The Contractor must employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

The Contractor must make the rules readily available to individuals requiring access to the information system describing users' responsibilities and expected behaviour with regard to information and information system usage. Rules of behaviour are to be based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users.

2 INFRASTRUCTURE ACCESS CONTROL *(MPS)*

All MPS endpoints including mobile devices must be managed by GC and/or the Contractor.

The Contractor must implement all appropriate measures to prevent bridging the GC network with external wireless services.

3 ACCESS CONTROL FOR TRANSMISSION MEDIUM *(MPS)*

The Contractor must:

a. control physical access to the Service Delivery Portal for the MPS and transmission lines within the Provider facilities;

b. protect telecommunications equipment, cabling and relays transceiving MPS Data or supporting services from interception or damage and design with redundancies, alternative power source and alternative routing;

c. protect telecommunications cabling from unauthorized interception and damage; and

d. control access to telecommunications wiring, spaces and pathways (i.e., telecommunications rooms, main terminal rooms and other equipment rooms).

4 ACCESS CONTROL POLICY AND PROCEDURES *(MPS)*

The Contractor must demonstrate the access control policies and associated access control requirements for Managed Print Service (MPS) components are in place.

The Contractor must demonstrate the current procedures for the management of accounts of Contractor Resources and Personnel for the MPS components are in place.

5 ACCESS ENFORCEMENT

The MPS must only allow authorized entities (users or processes) logical access to the system, applications, devices, files, security-relevant Data and other resources in accordance with applicable access control policies. The access control must comply with SSC Logical Access Control Standards (http://service.ssc-spc.gc.ca/en/policies_processes/policies/logical-v2). ***(MFD & MPS)***

The Contractor must implement all appropriate measures to prevent a data breach and must not disclose access to any GC related or GC specific information or data without the written permission of SSC or the D-A.

The Contractor must immediately notify SSC and/or the DA in writing of any actual or suspected unauthorized access to GC systems, Data, information or Infrastructure**.**

6 ACCESS RESTRICTIONS FOR CHANGE *(MPS)*

The Contractor must permit only qualified and authorized individuals to access information systems for purposes of initiating SSC and/or D-A approved changes, including upgrades and modifications.

The Contractor must maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should SSC and/or the D-A and the Contractor discover any unauthorized changes.

The MPS must enforce access restrictions for system changes and support auditing of the enforcement actions.

The Contractor must review information system changes quarterly to determine whether unauthorized changes have occurred.

7 ACCOUNT MANAGEMENT

The MPS must logout Users after a set period of inactivity determined by SSC and/or the D-A. The value of the time period must be configurable. ***(MPS)***

The MPS must logout privileged users (Contractor Administrators and GC Administrators) after a set period of inactivity set by SSC and/or Department or Agency (D-A) . ***(MFD & MPS)***

The Contractor must manage MPS privileged Operators, Administrators and User Accounts as follows:

a. create and manage all account types in accordance with role-based access profiles that specify privileges; ***(MFD & MPS)***

b. Multi-Function Devices (MFD) must have the capability to assign Users to roles that distinguish Users who can perform administrative functions from Users who perform User non-privileged functions. ***(MFD)***

c. track and monitor Operator, Administrators and User role assignments ***(MPS)***, and

d. adjust role assignments as Operator, Administrators and User role changes. ***(MPS)***

8 APPLICATION PARTITIONING *(MFD & MPS)*

The MPS and Print Devices must:

a. Separate user functionality (including user interface services) from Infrastructure management functionality; and

b. Prevent the presentation of Infrastructure management-related functionality at an interface for general (i.e., non-privileged) users.

Service Delivery Portal, MPS and Print Devices must isolate management and security functions from non-privileged Users and non-security functions. For example, these can be done by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods (e.g., using a logical separation, web administrators would use 2-factor authentication and normal users of the web application would use username/password authentication). Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

9 AUDIT REVIEW, ANALYSIS, AND REPORTING *(MPS)*

The Contractor must implement an audit review process that includes:

a. defining the level of auditing and identify personnel responsible for reviewing audit logs;

b. review and analysis of the MPS audit records annually and within agreed upon Federal Government Working Days of a request by SSC and/or the D-A for indications of inappropriate or unusual activity;

c. report findings of the audit review process to SSC within agreed upon Federal Government Working Days of completion of the audit, and

d. adjust the level of audit review, analysis, and reporting when there is a change in risk or as requested by SSC.

10 AUDITABLE EVENTS

The MPS must log all communications for each print Job including but not limited to the following as approved by SSC and/or the D-A ***(MPS)***:

a. date and time of print Job;

b. sender IP address

c. recipient printer IP address

d. sending hostname;

e. Transport Layer Security (TLS) usage;

f. Print Job ID; and

g. Username.

The MPS and Service Delivery Portal must log and audit the following privileged user/process events at a minimum. Any exception must be approved by the GC ***(MFD & MPS):***

a. Successful and unsuccessful attempts to access, modify, or delete security objects (Security objects include audit data, system configuration files and users' formal access permissions.)

b. Successful and unsuccessful logon attempts

c. Privileged activities

d. Starting time for user access to the system

e. All program initiations

In addition, the information system must audit the following unprivileged user/process events at a minimum. Any exception must be approved by the GC ***(MFD & MPS)***:

a. Successful and unsuccessful attempts to access, modify, or delete security objects

b. Successful and unsuccessful logon attempts

c. Starting time for user access to the system

d. Information on the source IP

The Contractor must inform SSC and/or the D-A of new auditable events and coordinate auditing process for logging of new events. ***(MFD & MPS)***

11 AUTHENTICATOR FEEDBACK *(MFD & MPS)*

The MPS components and the Print Devices must obscure feedback of authentication Data (e.g., masking password fields) during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

12 BASELINE CONFIGURATION *(MPS)*

The Contractor must demonstrate the current baseline configuration of the MPS components. Baseline configurations include information about information system components (e.g., standard software packages installed on servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. The baseline configuration should also demonstrate that all unused ports, services and software have been disabled and are using a hardened configuration (e.g., guest accounts deactivated, access control to all system files and directories applied, default passwords changed). The operating system on the Contractor's Service Delivery Portal is also considered a configuration item.

The Contractor must review and update the baseline configuration of the MPS:

a. When required due to incident or configuration item change; and

b. As an integral part of the MPS component installations and upgrades.

In order to limit potential exploits, the service and device's default administrator user identifier and password must be modified with complex passwords during initial configuration and installation. ***(MFD & MPS)***

13 BOUNDARY PROTECTION *(MPS)*

The Contractor must locate the Service Delivery Portal for the MPS physical components and related assets in a secure area. The secure area must have physical security controls allowing access only to authorized Contractor personnel.

14 COMMON CRITERIA *(MFD)*

The Common Criteria Protection Profile for Hardcopy Devices (Version 1.0, September 10, 2015, IPA, NIAP, and the MFP Technical Community) must be applied when procuring new MFDs. MFDs must be certified in compliance with the Hardcopy Devices Protection Profile. The main elements of the Protection Profile appendices must be utilized for Security Testing and Evaluation (ST&E) testing during the security assessment and authorization process as the test cases provided will garner artefacts for review.

Canada understands the industry is still transitioning to a HCDPP certification therefore the Offeror must provide MFD devices certified within the HCDPP documentation of 2015 as of August 31, 2019. After August 31, 2019, only HCDPP compliant MFD devices will be accepted.

Prior to August 31, 2019,

1. Canada will extend its acceptance to devices that are in the process of being HCDPP certified but have not yet been completely evaluated, with the caveat that further review will be required to validate full HCDPP compliance.
2. Canada will allow IEEE 2600.2 certified devices provided that the following key security areas are demonstrated as compliant by the Offeror using the test cases provided in annexes of the HCDPP or through a test plan and attestation accepted by GC:

a. Fax security elements must demonstrate there is not a capability to bridge to the network;
b. Overwrite capability for individual transactions must be the same as the HCDPP levels;
c. Encryption is limited to specific encryption levels and that these all meet the CSE approved strengths. Other encryption strategies will not be considered acceptable;
d. Ensure that specific requirements regarding secure communication (TLS/HTTPS/IPSEC/SSH) are in place;
e. Ensure that the entropy provided for the key generation process is sufficient and justified as per the HCDPP (appendix E);
f. Ensure the details regarding Key management are documented and presented as per the HDCPP (appendix F);
g. Ensure that key zeroization is an available and enabled feature; and
h. Demonstrated assurance of the RBAC capabilities of the devices to demonstrate separation between technician or repair mode in relation to device configuration and the configuration of accounts and processed data; and,
i. Other criteria under the HCDPP Protection Profile if requested by the GC.

15 CONFIGURATION CHANGE CONTROL *(MPS)*

The Contractor must support configuration management processes for the MPS including:

a. determining the types of changes that are configuration controlled;
b. approving configuration-controlled changes with explicit consideration for security impact analyses;
c. documenting approved configuration-controlled changes;
d. retaining and reviewing records of configuration-controlled changes;
e. auditing activities associated with configuration-controlled changes;
f. developing procedures for the distribution, installation, and rollback of changes implemented for a MPS release; and
g. testing the new and changed software and hardware not using the production environment.

16 CONFIGURATION MANAGEMENT PLAN *(MPS)*

The Contractor must provide a Configuration Management Plan that:

a. addresses roles, responsibilities, and configuration management processes and procedures;
b. defines the Configuration Items for MPS when the Configuration Items are placed under configuration management;
c. establishes the means for identifying Configuration Items throughout the system development life cycle and a process for managing the configuration of the Configuration Items;
d. defines a capability for a Malware Protection capability (Anti-virus) to:

i. automatically update malicious code protection mechanisms, including signature definitions;

ii. perform scans of the Infrastructure (servers, desktops and laptops)

iii. quarantine malicious code in response to malicious code detection.

e. defines the processes for patch management of the MPS that includes:

i) ensuring the most appropriate version of firmware, applications and operating systems are used as per the latest risk assessment;

ii) ensuring that vulnerabilities are evaluated and the Contractor-supplied security patches are applied in a timely manner;

iii) prioritizing critical patches using a risk-based approach; v) aligning criticality levels for patches as specified by SSC and/or the D-A;

iv) rating of vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v2;

v) testing and verification methodology to ensure that patches have been implemented properly;

vi) notifying SSC and/or the D-A of configuration vulnerabilities that would allow an unauthorized individual to compromise the confidentiality, integrity, or availability of MPS;

At a minimum, the MPS Change Management Plan must contain the following information:

a. The contractor's Change management authorities;

b. Contractor staff's roles and responsibilities;

c. How the Contractor will use the Change management process to support the development of the MPS IT service (e.g., a concept of operation);

d. The method used to uniquely identify the configuration items;

e. Configuration Item identification;

f. A description of the Change management process, including the Change review and approval process;

g. The measures used to enforce only authorized changes; and

h. The procedures that the Contractor will use to accept modified or newly created configuration items.

17 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES *(MPS)*

The Contractor must demonstrate to the D-A and/or SSC, evidence of the following:

a. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

18 CONFIGURATION SETTINGS *(MPS)*

The Contractor must manage configuration settings for the MPS that include:

a. specifying configuration settings to implement least privilege/functionality;

b. documenting exceptions to configuration settings, and

c. monitoring and controlling changes to the configuration settings in accordance with the Change Management and Configuration Management processes.

19 CONTENT OF AUDIT RECORDS *(MFD & MPS)*

The Print Device, MPS (including Service Delivery Portal) audit records must include the following log events unless otherwise approved by SSC and/or the D-A:

a. what type of audit event occurred;
b. when (date and time) the audit event occurred;
c. where the audit event occurred;
d. the audit source of the event;
e. the outcome (success or failure) of the audit event;
f. the identity of any user/subject associated with the audit event; and

The Contractor is to work with SSC and/or the D-A to determine what additional audit events may be required in the future.

The MPS and MFDs must perform capacity management on the audit record storage by:

a. keep 3 months of events and logs online;
b. keep events and logs associated with a security Incident for at least 2 years;
c. allocating enough audit record storage capacity;
d. configuring auditing to prevent storage capacity being exceeded;
e. alerting the Operator when the allocated audit record storage volume reaches 75% of the audit record storage capacity; and
f. overwriting the oldest audit records if storage reached maximum capacity.

The MPS and Multi-Function Devices on GC premises must provide the ability to off load audit records in real-time to an SSC and or D-A audit and logging system. This capability must include the ability to securely transmit audit logs in near real-time to a central logging system (e.g. SSC's Security Information and Event Management System) in a format and including content agreed to between SSC and the Contractor. Such functionality must be implemented by the Contractor within 60 Federal Government Working Days of a request by SSC, and have the capability to protect log information from unauthorized disclosure or alteration while in transit to the central logging system.

20 CONTINGENCY PLAN *(MPS)*

The Contractor must demonstrate evidence of a continuity plan for the MPS in GC premises, that is coordinated and communicated with personnel involved in supporting the plan, and must at a minimum:

a. Identify a detailed plan and documented process for restoring MPS;
b. Describes back up strategies for datacenter facilities, network facilities, operational support systems and data, and key service components;
c. Plans for transferring operational, management and administration functionality to a backup operations centre;
d. Plans for the resumption of essential missions and business functions within an agreed upon time period as approved by SSC and/or the D-A;
e. Provides recovery objectives, restoration priorities, and metrics;

f. Addresses contingency roles, responsibilities, and assigned individuals with contact information;

g. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented;

h. Addresses the necessary capacity planning required to ensure processing, telecommunications, and environmental support exists during contingency operations;

i. Describes the high level process for testing the continuity plan; and

j. Is reviewed and approved on an annual basis by the GC.

21 CONTROLLED MAINTENANCE *(MPS)*

The Contractor must perform controlled maintenance by:

a. Scheduling, performing, documenting, and reviewing records of maintenance and repairs on MPS components in accordance with manufacturer or the Contractor specifications;

b. Controlling all maintenance activities, whether performed on site or remotely, and whether the equipment is serviced on site or removed to another location;

c. Requiring that a designated GC authorized official explicitly approve the removal of the MPS components from the Service Delivery Point for off-site maintenance or repairs;

d. Ensure equipment and associated media is sanitized (data permanently deleted to an unrecoverable state) as approved by SSC and/or the D-A prior to removal from organizational facilities; and

e. Checking all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

22 CREDENTIAL MANAGEMENT

Access to the Service Delivery Portal must be secured to Authorized End Users.

The Contractor must provide and manage the credentials (authenticators) for End User and contractor personnel access to the Service Delivery Portal. The Contractor must also:

a. manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

b. manage information system authenticators by establishing initial authenticator content for authenticators;

c. manage information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. manage information system authenticators by establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

e. manage information system authenticators by changing the default content of authenticators prior to information system installation;

f. manage information system authenticators by establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

g. manage information system authenticators by changing/refreshing authenticators based upon a defined time period by authenticator type;

h. manage information system authenticators by protecting authenticator content from unauthorized disclosure and modification;

i. manage information system authenticators by requiring individuals implement, specific security safeguards to protect authenticators;

j. manage information system authenticators by changing authenticators for group/role accounts when contractor personnel membership to those accounts changes; and

k. not allow unencrypted static authenticators to be embedded in the systems, applications or access scripts and function keys.

23 CRYPTOGRAPHIC MODULE AUTHENTICATION *(MFD & MPS)*

Any use of cryptographic modules for authentication within the MPS and/or MFDs must use CSE approved cryptography (https://www.cse-cst.gc.ca/en/node/1831/html/26515).

24 DATA DELETION *(MPS)*

The Contractor must permanently delete specified MPS Data, upon request by SSC and/or the D-A as per CSE approved guidance (such as ITSG-06). The Contractor must also provide SSC and/or the D-A with evidence (such as a certificate of destruction) that the specified MPS Data was deleted.

25 DATA PROTECTION *(MPS)*

System Data and User Data must remain on GC premise and cannot be stored or accessed externally to the GC unless approved in writing by SSC and/or the D-A.

The Contractor may use external Contractor facilities for Service Management Data according to the following conditions as approved by SSC and/or the D-A:

a. must be segregated (logically or physically) from other non-GC Client's Data. The method of separating the GC data from other clients data is to be determined by the Contractor;

b. must not contain information labeled as Protected B or Classified;

Please see the definitions related to this requirement below:

System Data is the data that the Contractor uses to control or modify the operation, administration and management of the Print Management Solution and the Device Management solution which includes information on:

a) security Incidents and security alarms and events;

b) security information and events management (SIEM);

c) network perimeter management (e.g. firewall);

d) intrusion and prevention management;

e) malware protection and security controls;

f) hypervisor and virtual machine systems management;

g) network management and operations;

h) system configuration files, logs and scripts;

i) authentication, authorization and accounting systems;

j) disk systems;

k) capacity and resource management systems;

l) software distribution, updates and patches; and

m) Directory Services.

User Data is the data related to user documents and records that are being scanned, faxed and printed as well as the associated user's account and directory data.

Service Management Data is the data derived from the operation, administration, management of the support services and invoicing:

a) Service Requests;

b) Incident Tickets (excluding Security Incident Tickets);

c) billing records and invoices at an organizational level;

d) asset records;

e) configuration records;

f) system performance, capacity and resource planning information;

g) details on devices status, error codes and events.

26 DATA SOVEREIGNTY *(MPS)*

All MPS components, Protected and Classified Information as well as Information as determined by SSC and /or the D-A for the MPS, must reside within the Geographic Boundaries of Canada including Canadian Consulates and Embassies abroad. Any Information must be approved by GC before it can be transferred outside of Canada and using already agreed upon formats.

a. All MPS and Data repositories containing protected or classified information must be housed within the Geographic Boundaries of Canada including Canadian Consulates and Embassies abroad;

b. The storage of media, for purposes of backup and recovery, or historical archiving, or any other purpose, must be housed within secure approved location(s) within the Geographic Boundaries of Canada;

c. All GC print Data and communication with Multi-Function Devices located in Canada or abroad (e.g. Canadian Consulates and Embassies), must travel through appropriately secured networks. Data in transit must not be saved or stored between their starting and end points; and

d. It is the intent of SSC and the D-A to ensure that unauthorised access to GC Data e.g. access that has not been expressly permitted by SSC and/or the D-A within the MPS (e.g. to comply with a foreign government's production order) does not occur.

The Contractor must ensure to the extent of the Contractor's ability that all domestic network traffic (meaning traffic initiated in one part of Canada to a destination or individual located in another part of

Canada) is routed exclusively through Canada as per the ITPIN from TBS. https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/policy-implementation-notices/direction-electronic-data-residency.html.

The following are examples on how Data Sovereignty requirements would be applied to the various data elements being collected and stored by the Contractors.

Data Field Examples	Must remain in Canada?	Protected?
***IP Address**	Yes	Yes
***MAC Address**	Yes	Yes
***Floor plan with mapped devices**	Yes	Yes
***Device location – Street address/building, Floor, Room**	Yes	Yes
Department/Agency name	No	No
Device location – City, Province, Postal Code	No	No
Billing address – Street, City, Province, Postal Code, Floor	No	No
Device Functions (copy, print, scan, fax)	No	No
Business Contact Info (Name, Phone, Email)	No	No
Client Asset Number	No	No
Serial Number	No	No
Manufacturer	No	No
Model Name	No	No
Client Assert Number	No	No
Networked	No	No
Meter Read/Impressions Count	No	No
fax number	No	No
Print queue name	Need to analyse on a case by case	Need to analyse on a case by case

Special instructions	Need to analyse on a case by case	Need to analyse on a case by case
Comments	Need to analyse on a case by case	Need to analyse on a case by case

*The first four data elements (IP Address, MAC Address, Floor plan with mapped devices, and Device location) are considered as sensitive information by GC. On an individual basis, certain pieces of information fit the definition of Protected A, while certain other ones fit the definition of Protected B. The potential aggregate of this data in a system makes it Protected B data.

Any other data elements not listed above, would need to be assessed on a case by case to ensure to comply with GC Data Sovereignty requirements and other GC security requirements and privacy legislations.

The information that are not required for specific invoice and/or basic service and fleet management are recommended to stay in Canada.

One of the examples of addressing GC Data Sovereignty requirement is that the contractor can apply null variables such as “location #1” and relate it to the device location at GC SSC building in XXX Street in Ottawa. In this case, “location #1” can be transferred while the detailed device location remain in Canada.

27 DEVICE IDENTIFICATION AND AUTHENTICATION *(MPS)*

The MPS must ensure that devices (including portable devices) are identified and authorized prior to being connected to the network.

28 DISPOSAL OR REMOVAL OF INFRASTRUCTURE AND DEVICES *(MFD & MPS)*

The disposal or removal of WTD Print Service Infrastructure, Print Devices, MFDs or other Devices from GC locations must be carried out in compliance with CSE security guidance on Clearing and Declassifying Electronic Data Storage Devices (https://www.cse-cst.gc.ca/en/node/270/html/10572).

Prior to disposal or removal of WTD Print Service Infrastructure, Print Devices, MFDs or other Devices from GC locations, the Contractor must track, control and verify media sanitization as follows:

a. testing sanitization equipment and procedures to verify correct performance;

b. performing media sanitization in compliance with ITSG-06 (https://www.cse-cst.gc.ca/en/node/270/html/10572) requirements;

c. recording media sanitization actions; and
d. requesting SSC and/or D-A approval prior to disposal and/or removal from a GC location.

29 DOCUMENT PROTECTION IN PRINTING, COPYING AND SCANNING *(MFD)*

The MFD must have the capability to protect the User's Document from unauthorized disclosure and alteration.

30 ENCRYPTION CAPABILITY *(MFD)*

The MFD must have encryption capability to encrypt document image Data in temporary storage (to reduce the "window" for a network attack) and to protect Data in the event of failure of the MFDs normal overwrite processes due to power loss or paper jam.

31 ERASE UNCLAIMED DOCUMENTS *(MFD &MPS)*

The MPS and Multi-Function Devices (MFDs) must have the capability to erase unclaimed documents after a pre-set or predetermined time set by SSC and/or the D-A.

32 ERROR HANDLING *(MPS)*

The MPS must:

a. Identify potentially security-relevant error conditions (e.g. security events);
b. Generate error messages that provide information necessary for administrators to take corrective actions without revealing sensitive information and potentially harmful information in error logs and administrative messages that could be exploited by adversaries; and
c. Reveal error messages only to authorized personnel without revealing sensitive information that could be used to infer or extrapolate a vulnerability with the system.

33 FACILITY SITE CLEARANCE *(MPS)*

The Contractor must hold or obtain from PWGSC CISD a Facility Security Clearance (FSC) with Document Safeguarding Capability (DSC) for the MPS and the Service Delivery Portal facilities that are outside GC premises, at a level specified in the Security Requirements Checklist (SRCL).

The Contractor managing and or supporting the MPS must obtain a Designated Organization Screening (DOS) by the Canadian Industrial Security Directorate CISD.

In addition departments may require additional Security screening for access (physical or logical) to the MPS.

34 FAIL IN KNOWN STATE *(MFD & MPS)*

The MPS and the Print Devices must maintain their configuration state (such as passwords, service settings etc.) after a power down or reboot.

35 FIELD-REPLACEABLE NON-VOLATILE STORAGE DEVICES *(MFD)*

The MFD must have the capability to protect documents or confidential system information that may be present in Field-Replaceable Non-volatile Storage Devices from exposure if such a device is removed from the MFD including the use of data encryption unless otherwise protected by alternative mechanisms approved by the GC.

36 GC DATA PROTECTION *(MPS)*

The MPS Contractor must address the security of D-A's information through all phases of its life cycle or the life cycle of the Printing Service to ensure that security requirements are identified and risks mitigated from the onset, security controls are reviewed, management authorization is provided before operation, and authorization is maintained through continuous monitoring of the security posture.

37 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) *(MFD & MPS)*

The MPS and the Service Delivery Portal must uniquely identify and authenticate Operators (or processes acting on behalf of Operators), Administrators and Users.

The MPS, and the Print Device must have capabilities to perform identification and authentication locally and/or by an external server (such as Active Directory, LDAP or Kerberos).

The user authentication must comply with CSE User Authentication Guidance (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.30.031v2-eng.pdf).

If required by a D-A, the Print Devices must meet the following requirements:

a. Users must authenticate at the device to initiate a print job, scan, or copy;
b. the Print Devices are able to authenticate the Users by presenting an RFID badge (site & device dependent);
c. the Print Devices are able to authenticate the Users to the device in another manner other than an RFID badge;
d. Users will authenticate using the enterprise directory service (typically Active Directory). Only Users with an active network directory account will be able to use the device. Local accounts on device must only be allowed in exceptional cases;
e. the Print Devices support connection to LDAPv3 (or newer) server for Active Directory authentication;

If required by the D-A, the MPS on GC premises must support Smart Card Authentication capability including installation of a smartcard reader drivers and smartcard reader (embedded or via USB cable). If Smart Card Authentication is enabled, then USB ports must be accessible to accept insertion of USB smartcard tokens.

The MPS on GC premises must utilize SSC and/or D-A defined replay-resistant authentication mechanisms for network access to privileged accounts. ***(MPS)***

38 INCIDENT HANDLING *(MPS)*

The Contractor must demonstrate an incident handling capability for security incidents in MPS and SDP that includes preparation, detection and analysis, containment, eradication, and recovery. Evidence of such a capability could include:

a. Coordination of incident handling activities with contingency planning activities.
b. Procedures related to:
   i) Incorporating lessons learned from ongoing incident handling activities into incident response, training, and testing/exercises; and
   ii) Implementing the resulting changes accordingly.

In the event of security incident, the Contractor may be requested by SSC and/or the D-A to create an Emergency Change Request:

i) within a time period specified by SSC and/or the D-A for each mitigation measure requested by SSC and/or the D-A to contain a Security Incident.

ii) based on severity as specified by SSC and/or the D-A for each mitigation measure requested by SSC and/or the D-A to contain a Security Incident and,

iii) must implement the Emergency Change Request in accordance with SSC and/or the D-A priority level.

The Contractor must define appropriate actions to take in response to incidents based on the severity and category to ensure continuation of the service.

a. The Contractor must initiate response procedures to security incidents based on severity as specified by SSC and/or the D-A

b. The Contractor must report all suspected or actual privacy and security violations via phone or email (in an agreed upon frequency) for the MPS to SSC and/or the D-A following guidelines in the GC Cyber Event Management Plan (https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html).

The Contractor must implement a response capability for information spillage security incidents that includes:

a. Identifying the specific information involved in the information system contamination;

b. Responding to information spills by alerting appropriate GC personnel, isolating the contaminated MPS components, eradicating the information from the contaminated components, and identifying other information systems or MPS components that may have been subsequently contaminated; and

c. Providing information spillage response training to assigned Administrators.

39 INCIDENT MONITORING *(MPS)*

The MPS must implement incident procedural and administrative monitoring to detect attacks and unauthorized use of the MPS. This includes mechanisms (e.g. procedural and administrative activities) approved by SSC to assist in the tracking and documenting of security incidents and in the collection and analysis of information.

40 INCIDENT REPORTING *(MPS)*

The Contractor must provide security incident reporting and mitigation mechanisms, including, but not limited to:

a. Generating warnings or reports on system activity based on security parameters;

b. Terminating access and/or generating a report when potential security violations are detected;

c. Preserving and reporting specified audit Data when potential security violations are detected; and

d. Providing all evidence associated with a Security Incident to SSC and/or the D-A.

41 INCIDENT RESPONSE POLICY AND PROCEDURES *(MPS)*

The Contractor must demonstrate evidence of a formal, documented policy, procedure and plan to facilitate the implementation and maintenance of security incident response activities. The Contractor must comply with the GC SOC Incident Handling procedures.

42 INFORMATION OUTPUT HANDLING AND RETENTION *(MPS)*

The MPS must handle and retain information within the system and information output from the system in accordance with applicable D-A legislation and TBS directives on record keeping (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16552) and the TBS Policy on Information Management (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742).

43 INFORMATION SYSTEM COMPONENT INVENTORY *(MFD & MPS)*

All devices must be recorded and tracked within a designated asset repository. Contact information for the device's responsible authority must be recorded in the requisite asset repository. Device identifiers must be unique and recorded with appropriate owner, configuration, location, and usage information. All information must be kept current and accurate.

The Contractor must provide a list of the MPS components installed in GC premises that includes all hardware and software that:

a. accurately reflects their current configuration;

b. is at the level of granularity deemed necessary for tracking and reporting;

c. includes enough information to achieve effective property accountability;

d. is available for review and audit by SSC and/or D-A, and

e. is updated as an integral part of component installations, removals, and SSC and/or D-A MPS updates.

44 INFORMATION SYSTEM COMPONENT INVENTORY *(MPS)*

The Contractor must demonstrate a MPS configuration for approval by SSC and/or the D-A. The Contractor will only deploy the assessed/approved components and configurations.

The Contractor must request SSC and/or D-A approval for any deviations to current deployed configurations in the MPS component inventory.

45 LEAST FUNCTIONALITY *(MFD & MPS)*

The Contractor must ensure that the MPS components and applications are installed and maintained in a security-hardened configuration.

The Contractor must ensure the MPS and the Print Devices use only authorized features; and identify and disable features deemed as unnecessary and/or non-secure such as ports, protocols, and services (such as disable internet access and USB port).

The Contractor must employ a deny-all and permit-by-exception policy to allow the execution of only authorized software services on the MPS.

The Print Devices must support IP filtering and port blocking.

If required by a D-A, the MPS and the Print Device must meet the following requirements:

a. be able to restrict access to USB ports in either a logical or physical manner; physically prevent access to the USB if the USB port is used for authentication purposes;

b. not allow the MFD scanning to a USB drive and or SMTP; and

c. assign static IP addresses to the Print Devices.

46 LEAST PRIVILEGE *(MPS)*

The MPS must prohibit unauthorized privileged access and or functions by non-privileged Users to

WTD Print Service Infrastructure and devices. The Contractor must implement Role Based Access Control (RBAC) with proper group policies (GPO) to ensure unauthorized or non-privileged Users are not able to access and or execute privileged information or functions.

The Contractor is to employ the principle of least privilege, allowing only authorized access for Users (or processes acting on behalf of Users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

The Service Delivery Portal must have an access control mechanism to the MPS Data that limits the Administrator or User from a D-A to the data of its D-A only. For example, the Department_1 Administrator or User can only access the Department_1 information and cannot access to the information from the other Departments.

47 MAINTENANCE PERSONNEL *(MFD & MPS)*

The Contractor must demonstrate evidence of a process for maintenance personnel authorization;

> The Contractor must maintain a current list of authorized maintenance organizations or personnel;
>
> The Contractor must ensure that personnel performing maintenance on the printing Service or devices have required access authorizations;
>
> In the event maintenance personnel do not possess the required access authorizations, the maintenance activities must be supervised by designated authorized personnel with required access authorizations and technical competence deemed necessary

48 MAINTENANCE TOOLS

The use of the maintenance tools for MPS must be approved by SSC and or the D-A. Prior to removal, any maintenance tools or associated media must be checked by SSC and or the D-A. Any tool or media found to contain GC information must be sanitized, destroyed or explicitly authorized for removal by the GC.

49 MEDIA ACCESS *(MPS)*

The Contractor must restrict access to IT media (digital and non-digital) containing MPS Data to authorized Administrators.

The Contractor must control and securely store sensitive data on any IT media (digital and non-digital).

The MPS must control and protect information system media during transport using an identified custodian in accordance with RCMP G1-009 transport and transmittal guidance.

50 MEDIA SANITIZATION *(MPS)*

The Contractor must perform information system media sanitization, on both digital and non-digital media prior to disposal or reuse, whether or not the media is considered removable.

The Contractor must not remove any Information system media (digital and/or non-digital) regardless of whether or not the media is considered removable from D-A premise, until it has been sanitized by the Contractor and approved by SSC and/or the D-A.

Media sanitization must be performed and documented as per the Communications Security Establishment (CSE) of Canada IT Security Guidance ITSG-06 ((https://www.cse-cst.gc.ca/en/node/270/html/10572; DoD 5502 overwrite equivalent, minimum of 3x overwrite using an SSC and/or D-A approved overwrite utility).

51 MONITORING PHYSICAL ACCESS *(MPS)*

The Contractor must monitor physical access to the Service Delivery Portal for the MPS for unauthorized access by

a. monitoring in real-time physical intrusion alarms and surveillance equipment;

b. recording all physical access events;

c. providing logs when requested by SSC and or the D-A;

d. creating a Security Incident upon discovery of abnormal activity;

52 NETWORK MONITORING *(MPS)*

The ability for the GC to monitor and perform traffic analysis is required in regards to WTD Print services. The exact implementation of the network monitoring capability will be dependent on the proposed architecture* in relation to the Contractor management elements as well as use and maintenance of the Service Delivery Portal. Of note, this may require installation of sensors, provided as Government Furnished Equipment (GFE), to enable a sustained network capture of all Internet Protocol (IP) Layer network traffic and interactions between Canada and the WTD Print Service with the ability to inspect within encrypted traffic when communicating to and from the Internet or any other Network Interconnection points. The Contractor must not make any modifications to the network monitoring measures to SSC equipment located at each Service Delivery Point (SDP) without approval from SSC. Additionally, Canada reserves the right to install, or request that the Contractor installs on its behalf, for network monitoring purposes, Canada developed software applications on computer/communications systems, including, but not limited to, workstations, servers, mobile devices and networking equipment.

* Note: Should the proposed architecture be deemed to require the installation of sensors, Canada developed software applications or other GC monitoring equipment at Contractor facilities, the Contractor will be provided with an opportunity to submit an alternate architecture for consideration or otherwise must accept the monitoring system deployment stipulated by Canada.

53 NON-LOCAL MAINTENANCE *(MPS)*

The MPS must support non-local maintenance and diagnostic activities (i.e. remote management over a network) to support life cycle management within the Infrastructure to maintain (i. e. component repair/upgrade, license file updates, etc.) the assets within the environment without requiring console access within GC datacentres. This includes:

a. Approving and monitoring non-local maintenance and diagnostic activities;

b. Allowing the use of non-local maintenance and diagnostic tools as approved by SSC and/or the D-A and as documented in the security plan for the MPS which must include the policies and procedures for the establishment and use of non-local maintenance and diagnostic connections.

c. Permitting the use of LoA3 authenticators (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.30.031v2-eng.pdf) in the establishment of non-local maintenance and diagnostic sessions;

d. Obtaining approval and notifying appropriate personnel of each nonlocal (remote) maintenance session;

e. Maintaining, reviewing and auditing the records for non-local maintenance and diagnostic activities;

f. Permitting the use of cryptographic mechanisms to protect the integrity and confidentiality of nonlocal (remote) maintenance and diagnostic communications;

g. Restricting the privileges of accounts used for nonlocal maintenance to the minimum that are required; and

h. Ensuring that accounts used for non-local (remote) maintenance are disabled whenever they are not in use.

54 NON-PRODUCTION ENVIRONMENT *(MPS)*

The Contractor must separate (through logical or physical means) production and non-production environments (such as development and test environments) and enforce separation with access controls to prevent unauthorized access or changes to information assets.

Any connectivity between non-production and production environments must be authorized and must be accurately and completely documented to identify required functionality and security controls allocated to maintain the level of protection commensurate with the sensitivity of the information.

The Contractor must not use production data for testing or development.

55 PASSWORD-BASED AUTHENTICATION *(MPS)*

When PASSWORD-BASED authentication for End Users is used to access the Service Delivery Portal and the MPS:

a. The information system, for password-based authentication, enforces minimum password complexity based upon GC-approved requirements for case sensitivity, number of characters, mix of upper-case letters/ lower-case letters, numbers, and special characters, including minimum requirements for each type (e.g. at least 8 characters, at least three of the following character groups: upper case, lower case, number, and special character);

b. The information system, for password-based authentication, enforces the predefined number of changed characters when new passwords are created;

c. The information system, for password-based authentication, stores and transmits passwords that have been protected using CSE approved cryptography (ITSP.40.111, see https://www.cse-cst.gc.ca/en/publication/list/Cryptography);

d. The information system, for password-based authentication, enforces password minimum and maximum lifetime restrictions of GC-approved values for lifetime minimum (at least 1 day), lifetime maximum (e.g. 90 days);

e. The information system, for password-based authentication prohibits password reuse for a GC-defined number of generations; and

f. The information system, for password-based authentication that allows for the use of a temporary password for system logons must be followed by an immediate change to a permanent password upon initial logon.

Any exception to password-based authentication requirements must be approved by SSC and/or the D-A.

56 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION *(MFD & MPS)*

The MPS must prevent access to infrastructure components or resources without Identification, Authentication, and Authorization.

57 **PERSONNEL SCREENING *(MFD & MPS)***

The Contractor must ensure that all personnel is in compliance with personnel security clearance requirements as specified in the Security Requirement Check List (SRCL).

58 **PERSONNEL TERMINATION *(MFD & MPS)***

The Contractor must, upon termination of an individual's employment associated with the MPS:

a. terminate all access to the MPS for the employee, including remote access;
b. retrieve all security-related property (e.g., employee identity card, physical authentication token);and
c. notify Canadian Industrial Security Directorate (CISD) to terminate personnel screening designations.

59 **PERSONNEL PHYSICAL ACCESS CONTROL *(MFD & MPS)***

The Contractor must implement role-based physical access controls within the MPS by:

a. keeping an updated access list of personnel with authorized access to the facilities;
b. implementing separation of duties where the authorization to access facilities is done by a different person than the authorization to access MPS; and
c. allowing access to facilities to authorized personnel with an approved authorization credential.

60 **PKI-BASED AUTHENTICATION *(MFD & MPS)***

In the event PKI-BASED authentication for End Users is required to access the Service Delivery Portal, MPS and/or the MFD, the following requirements must be met:

a. The information system, for PKI-based authentication, validates certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
b. The information system, for PKI-based authentication, enforces authorized access to the corresponding private key;
c. The information system, for PKI-based authentication, maps the authenticated identity to the account of the individual or group; and
d. The information system, for PKI-based authentication, implements a local cache of revocation Data to support path discovery and validation in case of inability to access revocation information via the network.

Any exception must be explicitly approved by SSC and/or the D-A

61 **PREVIOUS LOGON (ACCESS) NOTIFICATION *(MPS)***

The MPS should notify the Administrators and Operators upon successful logon (access), of the date and time of the last logon (access), whenever technically possible and available as an option using existing products which do not require additional or customized solutions.

62 **PROTECTION OF AUDIT INFORMATION *(MFD & MPS)***

The MPS and the MFD must:

a. protect audit information from unauthorized access, modification, and deletion;

b. use tamper resistant cryptographic mechanisms to protect integrity of audit information when needed, and

c. backup audit records onto a different system or media than the system being audited on a schedule specified by SSC and/or the D-A.

The logs must be archived for a sufficient period of time to support regulatory and policy compliance audits. This includes:

a. store logs for at least 6 months and;

b. keep events and logs associated with a security Incident in MPS for at least 2 years.

63 PROTECTION OF INFORMATION AT REST *(MFD & MPS)*

The MPS and Multi-Function Devices (MFDs) must protect the confidentiality and integrity of GC data-at-rest (DAR) including using cryptographic solutions with CSE-approved cryptography (ITSP.40.111) and key management technologies and processes unless otherwise protected by alternative mechanisms approved by the GC. Integrity of GC Data must be maintained to prevent and detect improper alteration, duplications, or destruction (e.g., double keying, message authentication, digital signature, check sums etc.)

64 PSTN FAX-NETWORK SEPARATION *(MFD)*

Any MFD with a fax function must conform to the fax requirements defined in the Protection Profile for Hardcopy Devices, Version 1.0, September 10, 2015, IPA, NIAP, and the MFP Technical Community. PSTN fax-network separation must ensure that the PSTN fax modem is not used to create a data bridge between the PSTN and the LAN. The MFD prohibits communication via the fax interface, except transmitting or receiving User Data using fax protocols. The test cases included in the Protection Profile (PP) appendices are to be utilized for Security Testing and Evaluation (ST&E) testing during the SA&A process. If required by a D-A, the fax function must not be integrated on the device until approval by SSC and/or the D-A.

65 PUBLICLY ACCESSIBLE CONTENT *(MPS)*

The Contractor must obtain SSC's approval before making any MPS content publicly available.

66 REMOTE ACCESS *(MPS)*

Any use of Remote Management of the MPS must take place using a method approved by SSC that includes:

a. Remote Management be restricted to MPS locations approved by Government of Canada (GC) and have dedicated management consoles.

b. Documenting allowed methods of Remote Management and establish usage restrictions and implementation guidance for each allowed remote management method;

c. monitoring for unauthorized Remote Management;

d. authorizing Remote Management prior to connection;

e. employing automated mechanisms to facilitate the control and monitoring of Remote Management methods;

f. routing all Remote Management to MPS through a limited number of managed access control points;

g. protecting information about Remote Management mechanisms from unauthorized use and disclosure;

h. implementing cryptography mechanisms to protect the confidentiality and integrity of information within the remote access session.
i. All Remote management connectivity must be logged and the GC must have visibility into the unencrypted traffic.

The Contractor must authorize the execution of privileged commands and access to security-relevant information via remote access for the management of MPS as approved by SSC and/or the D-A.

In the event the remote access is provided by the Contractor, the Contractor must meet the following requirements as approved by SSC and/or the D-A:

a. two factor authentication (2FA);
b. Detailed access and system logging feeding Contractor and/or GC SIEM (Security Information and Event Management) system as determined by SSC and/or the D-A;
c. full session auditing for all privileged access and storing records for 90 calendar days;
d. dedicated hardened end point (workstation or laptop) as approved by SSC and/or the D-A;
e. documented allowed methods of remote management, implementation guidance and usage restrictions;
f. monitoring for unauthorized access;
g. a secure session connection utilizing an accepted level of encryption as per CSE standards such as SSL/TLS 1.2 or VPN; and
h. Remote Access solution designs must adhere to CSE approved network zoning requirements ITSG-22 and ITSG-38.

67 SECURE CONFIGURATION *(MFD)*

The MFD must have the capability to protect its security settings from unauthorized disclosure and alteration when they are stored in the MFD and in transit to or from an external IT entity. The MFD also must have the capability to protect the on-board dip switches that allows Users to reset/turn-off some of the security features like encryption, job-wipe on successful print, etc.

68 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES *(MPS)*

The Contractor must monitor, disseminate, and respond to security alerts, advisories, and directives from designated external organizations (e.g. SSC, the Canadian Cyber Incident Response Centre (CCIRC)) on an ongoing basis and must implement security directives in accordance with established time frames and notify the GC of the degree of non-compliance.

69 SECURITY AWARENESS *(MPS)*

The Contractor must demonstrate evidence of security awareness and training for MPS personnel as follows:

a. as part of initial training for new personnel
b. before authorizing access to the MPS or performing assigned duties;
c. annually and when security impacting changes to the printing Service occur;
d. Training based on personnel roles, and responsibilities; and
e. The organization retains individual personnel training records for a length of time determined by SSC and/or the D-A.

70 SECURITY INCIDENT *(MPS)*

In the event of a security incident, or as otherwise requested by SSC and/or the D-A, the Contractor must cooperate with any security audits or inspections requested by SSC and/or the D-A by providing requested information in a timely manner, based on severity as specified by SSC and/or the D-A.

The Contractor must provide an annual summary security reports to SSC and/or the D-A to include Reports related to the number, severity, and mitigations for security incidents.

71 SECURITY REVIEW *(MPS)*

a. On an annual basis, the Contractor must perform a conformance review to ensure that security requirements are being met.
b. The Contractor must provide the findings of their conformance review in the form of a report along with supporting evidence for SSC and/or D-A review within a period of time agreed to by both SSC and/or the D-A and the Contractor.
c. If SSC and/or the D-A deems that the evidence does not support the conformity to the contract then the Contractor must supply a plan that addresses the deficiencies identified by SSC and/or the D-A.

72 SENDING AND RECEIVING PSTN FAXES *(MFD)*

When sending and receiving PSTN faxes, the MFD must have the capability to protect the User's Document from unauthorized disclosure and alteration while the document is in transit and when it is stored in the MFD.

73 SEPARATION OF DUTIES *(MPS)*

The Contractor must:

a. Separate duties of individuals by division of roles and responsibilities to reduce the possibility for a single individual to compromise a critical process and to ensure that personnel are performing only authorised duties relevant to their respective jobs and positions;
b. Document separation of duties of individuals; and
c. Define information system access authorizations to support separation of duties.

74 SESSION AUTHENTICITY *(MFD & MPS)*

The MPS must establish and maintain the authenticity of communication sessions for each session by recognizing only system-generated unique session identifiers and invalidating session identifiers upon logout or other session termination.

75 SESSION LOCK *(MFD & MPS)*

The MPS must prevent further access to the system by initiating a device session lock after an approved time period by SSC and/or the D-A, of inactivity or upon receiving a request from a user. Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. This is typically at the operating system level, but can also be at the application level.

The information system must retain the session lock until the user re-establishes access using established identification and authentication procedures.

Session Lockout: After a specified period of inactivity, computing devices such as MFDs, servers, workstations or laptops must be configured to lock after a specified period of inactivity, and require the user to enter their password to unlock the device.
The information system session lock mechanism, when activated on a device with a display screen, must place a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.

The value of the time period must be configurable. If there is no device session lock capability or the defined time period is a fixed time in some operating systems or applications used by the MFD or MPS, SSC will need further risk analysis in order to approve their uses in the MPS. Any exceptions regarding device session lockout capability must be reviewed and approved by SSC and/or the D-A.

76 STORAGE SANITIZATION IN JOB BASED DEVICES *(MFD)*

The MFDs must have ability to secure-erase Print Data between print jobs. This must ensure that Print Data is permanently unrecoverable by any means. Automatic three passes (3X) or higher overwrite must be configured to operate and execute after every Print Job for each specific Print Device including MFDs and other imaging devices. If a 3X overwrite cannot be performed the Contractor must propose an alternate solution for SSC and/or the D-A's review and consideration.

77 SUPPLY CHAIN / ACQUISITION PROCESS *(MPS)*

The Contractor must be compliant with SSC Supply Chain Security Information Assessment Process for the products used for the MPS. The Contractor must use evaluated products only.

At any time during the Contract, if the Contractor proposes introducing new commercial products, on the GC network, on the Contractor's Infrastructure, on a third party Infrastructure, and if these products will be interconnected with GC network, the Contractor must first obtain the written approval of both the D-A and SSC. This includes any new commercial products that were not on the IT Products List approved by both the D-A and SSC in accordance with supply chain integrity checks in the Supply Chain Threats to the Government of Canada - Equipment Approval letter. SSC and/or the D-A reserves the right to refuse new commercial products, propose new safeguards and to independently validate and approve the commercial products if these products will be used on or interconnected with the GC’s network.

At any time, if SSC and/or the D-A notifies the Contractor that any given manufacturer or OEM is no longer considered a trusted manufacturer or OEM (i.e. un-trusted), the Contractor must immediately cease deploying equipment made by that manufacturer or OEM in the GC’s network and in any Infrastructure of the Contractor that will interconnect with GC’s network. For already deployed equipment, the Contractor has to identify and/or remove equipment made by that manufacturer or OEM in GC’s network and in any Infrastructure or backbone of the Contractor that will interconnect with GC's network.

If the Contractor becomes aware that any third party is deploying un-trusted equipment on its network, the Contractor must immediately notify both the D-A and SSC.

78 TRANSITION SERVICES AT END OF CONTRACT PERIOD

As applicable, either at the end of contract term, at the end of the final option term, or upon termination, at D-A written request, the Contractor must transfer, using a secure mechanism approved by SSC and/or the D-A all MPS Data and Metadata to SSC or the D-A in an accessible, machine-readable and usable form acceptable to SSC and/or the D-A at no additional cost to the Crown within 40 calendar days of a request by SSC and/or the D-A or such longer period as the parties may agree. The Data and Metadata will be considered received upon sign-off by SSC and/or D-A. The sign-off will certify that the data and metadata that has been received is accessible, machine-readable and usable by SSC and/or the D-A

As applicable, either at the end of contract term, at the end of the final option term, or upon termination, SSC and/or the D-A may request the Contractor to remove the MPS including all hardware and software owned by the Contractor and installed in MPS at no additional cost to the D-A within 40 FGWDs of a request by SSC and/or the D-A. Upon failure of the Contractor to remove the MPS, SSC and/or the D-A may take ownership of the full MPS.

79 TRANSMISSION CONFIDENTIALITY AND INTEGRITY *(MFD & MPS)*

The MPS and Print Devices must provide end-to-end confidentiality and integrity of data-in-transit including the use of cryptographic solutions by the CSE (ITSP.40.111) with CSE-approved cryptography and key management technologies and processes. This includes:

a. protecting Data transmitted between components and between authorized systems to ensure that information is intact and that the Data has not been changed in transit, either due to malicious intent or by accident;

b. providing the capability to perform source to destination file integrity checks for exchange of Data and alert appropriate parties when an error condition occurs (either with a specific transmission or with systems components); and

c. Establishing trusted communication paths to ensure that communications with the Print Devices and MPS are performed with known endpoints.

80 UNSUCCESSFUL LOGIN ATTEMPTS *(MPS)*

The MPS, including the Service Delivery Portal and the Management Console must:

a. enforce a limit as approved by SSC and/or the D-A of consecutive invalid login attempts by a user for defined time period; and

b. automatically lock the account/session for a time period approved by SSC and/or the D-A and/or lock the account/node until released by an Administrator as specified by SSC or the D-A; and/or delay next login prompt according to a SSC and/or D-A approved delay, when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

81 USAGE AND CONFIGURATION AUDIT TRIAL *(MFD & MPS)*

All MPS components and MFD's must log Print Document transfers (including source and destination addresses) and date and time of transfer. In addition, all MPS components and MFD's must log resident application access for both successful and unsuccessful login access.

82 USE OF EXTERNAL INFORMATION SYSTEMS *(MPS)*

The Contractor must prohibit the use of external information systems to physically or logically connect to the MPS and the Print Devices.

83 VERIFYING MFD FUNCTION *(MFD)*

The MFD must check itself for malfunctions by performing a self-test each time that it is powered on.

84 VERIFYING SOFTWARE UPDATES *(MFD)*

The MFD must ensure that only authorized personnel are permitted to install software, and the MFD must have the capability to help the installer to verify the authenticity of the software update.

85 VULNERABILITY *ASSESSMENT (MPS)*

The Contractor must demonstrate that regular Vulnerability Assessments (VAs) are conducted at locations where the WTD Print Service systems are located outside of GC provided facilities.

At the discretion of the GC and if requested by the GC the Contractor must allow Vulnerability Assessment (VA) testing of the Service Delivery Portal, conducted by the GC or a third party selected by the GC on an annual basis within 20 Federal Government Working Days (FGWD) notice of such a request. The Contractor must determine the assignment of responsibility for supporting Vulnerability Assessment testing and provide all support required by the GC.

The GC or a third party acting on its behalf may conduct Vulnerability Assessment testing of WTD Print Service systems located inside and or outside of the GC and provide a VA Report to the Contractor that will identify the vulnerabilities that were detected. The Contractor must provide the GC with a Vulnerability Mitigation Report and implement the corrective measures identified within a time frame agreed to by the GC and the Contractor at no cost to the GC.

86 WIRELESS ACCESS *(MFD & MPS)*

Where under the responsibility of the contractor, the Contractor must disable all wireless networking functions internally embedded within MPS. This includes, but not limited to, disabling wireless functions in Servers, Service Management tools, Service Delivery Portal Servers, Print Devices and the Contractor technician tools that are physically or logically connected to WTD Print Service.

For certain situations as deemed necessary by the D-A, based on a risk assessment and approval by SSC and or D-A, wireless capabilities may be made available where all other alternatives for GC Infrastructure connectivity have been exhausted, or as requested by SSC or the D-A and the appropriate wireless security controls are implemented in compliance with CSE guidance (https://www.cse-cst.gc.ca/en/publication/list/Wireless-and-Mobility).

If required by a D-A, the MFDs may be required not to have any physical wireless and Bluetooth capability.

87 ZONING CAPABILITIES *(MPS)*

The MPS on GC premises must meet requirements set out by the Communications Security Establishment of Canada (CSE)’s IT Security Guidance (ITSG) document, Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22) (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg-22-eng.pdf).

Term	Definition
2FA	Two factor authentication is a method of confirming a user's claimed identity in which a user is granted access only after successfully presenting 2 or more pieces of evidence or factors to an authentication mechanism.
Administrator	A User that is authorized to perform administrative operations for the WTD Print Services. GC Administrator is an Administrator working for and managed by the GC and a Contractor/Service Provider Administrator is an Administrator working for and managed by the Contractor/Service Provider. Administrators generally perform configuration, maintenance and management activities for the service and typically require privileged access rights to the system.
Access Control	The processes of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities. It ensures individuals can only use those resources they are entitled to use and then only for approved purposes, enforcing security policies that govern access throughout the enterprise.
Authentication	The mechanism used to identify a user, usually by providing a username and a password, or other credentials. This ensures that the user is really who they claim to be.
Authorization (Security Assessment & Authorization)	The ongoing process of obtaining and maintaining official management decision by a senior organizational official to authorize operation of an information system and to explicitly accept the risk of relying on the information system to support a set of business activities based on the implementation of an agreed-upon set of security controls, and the results of continuous security assessment.
Availability	The state of being accessible and usable in a timely and reliable manner. Note: It is implicit in the definition that the integrity of objects being accessed has not been lost due to compromise (ex., corrupted information is not considered available, because it is not usable).
CISD	Canadian Industrial Security Directorate
CCIRC	The Canadian Cyber Incident Response Centre
Certificate	An public key certificate, in a format which is in accordance with ITU-T recommendation X.509 V3, as described in rfc5280(http://www.ietf.org/rfc/rfc5280.txt), which contains a public key of a subscriber, which can be an individual or a device, together with related information that is digitally signed with the private key of the Certification Authority that issued the Certificate.
Change Management	Standardized methods and procedures used for efficient and accurate handling of all changes to WTD Print Services, in order to minimize the number and impact of any related incidents to the service.
Common Criteria	Abbreviation for the Common Criteria for Information Technology Security Evaluation, an international standard for computer security certification. Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements through the use of Protection Profiles (PPs), vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims.
Compromise (noun)	The unauthorized access to, disclosure, destruction, removal, modification, use, or interruption of IT assets, causing a loss of confidentiality, integrity and/or availability.

Compromise (verb)	The act of causing a compromise by exploiting vulnerabilities. Note: A compromise may lead to the failure of a business activity and its related requirements. This failure may lead to injuries to national interests or non-national interests.
Confidentiality	The state of being disclosed only to authorized individuals. A characteristic applied to information to signify that it can only be disclosed to authorized individuals.
Configuration Management	Standardized methods and procedures for establishing and maintaining hardware and software configuration items of WTD Print Services.
Credential	An object or data structure that authoritatively binds an individual to a token possessed and controlled by that individual, which is used to authenticate or confirm an individual's identity.
CSE	Communications Security Establishment
Criticality	The relative importance of a business activity in promoting or maintaining the health, safety, security, or economic well-being of Canadians, or to the efficient functioning of the GC.
D-A	Department or Agency
Data	Electronic representation of information. The quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.
Data Centre	A facility used to house computer systems and associated components, such as telecommunications and storage systems.
Device	A physical object (e.g., a projector, whiteboard, computer/laptop, printer, scanner).
Digital Media	Any media that is encoded in a machine-readable format. Digital media can be created, viewed, distributed, modified and preserved on digital electronics devices.
Document	A medium and the information recorded on it that generally has permanence and can be read by a person or a machine.
DOS – Designated Organization Screening	A designated organization screening (DOS) allows organizations to get security screening for their personnel at the reliability status level.
Encryption	The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text. Source: http://www.webopedia.com/TERM/E/encryption.html
External Information Systems	Information systems or components of information systems that are outside of the authorization boundary of WTD Print Services. They include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (ex., hotels, train stations, convention centres, shopping malls, or airports); (iii) information systems owned or controlled by non-GC

	organizations that are not dedicated and authorized to interface with WTD Print Services within the GC network.
End User	A person that is authorized to use the WTD Print Service.
Field-Replaceable Non-volatile Storage Device	Is any Field-Replaceable Unit (FRU) for which the primary purpose is to provide non-volatile storage. It does not apply to storage devices that are a non-field-replaceable component of a larger FRU that is not primarily used for storage.
Firewall	A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.
FGWD	Federal Government Work Day
GC	Government of Canada
GC SIEM	Security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware. Source: https://en.wikipedia.org/wiki/Security_information_and_event_management
General User	An End User who is not a privileged User.
Geographic Boundaries of Canada	Geographic Boundaries of Canada refers to all locations within Canada as well as Canadian Consulates and Canadian Embassies.
GFE	Government Furnished Equipment
GPO	Group Policy is a feature of the Microsoft Windows NT family of operating systems that controls the working environment of user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. Source: https://en.wikipedia.org/wiki/Group_Policy
Harden	Securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one.
Hardware	A physical device or component such as a desktop, laptop, printer, monitor, physical storage device etc.
Identification	An action or a process of identifying a user or device or the fact of being identified.
Implementation	A term used to designate the phases of the system lifecycle that are responsible for the delivery of an information system. It includes the initiation, development/acquisition, and integration and installation phases of the system lifecycle, but excludes the operations and maintenance phase and the disposal phase.
Incident	Event which is not part of the standard operation of a Service and which causes, or may cause, an interruption to, or a reduction in, the quality of that Service.
Information (Information Assets)	Any pattern of symbols or sounds to which meaning may be assigned. It is that which informs. In other words, it is the answer to a question of some kind. It is thus related to data and knowledge, as data represents values

	attributed to parameters, and knowledge signifies understanding of real things or abstract concepts.
Information System	An information system is generally composed of data, computing platforms, communications networks, business applications, people, and processes, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Infrastructure	Set of hardware, software and networks required to support the WTD Print Service.
IP	The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying packets across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet. Source: https://en.wikipedia.org/wiki/Internet_Protocol
Integrity	The state of being accurate, complete, authentic, and intact. Note: Integrity is generally applied to information assets. Integrity can also be applied to business processes, software application logic, hardware and personnel.
Internet	Collection of interconnected networks and application servers that are publicly accessible worldwide and that are commonly referred to as the Internet.
Installation	The general installation services provided by the Contractor.
IT	Information Technology
IT Security	The discipline of applying security controls, security solutions, tools, and techniques to protect IT assets against threats from compromise throughout their lifecycle, based on the security category of supported business activities, and in accordance with departmental and GC policies, directives, standards, and guidelines.
IT security incident	Any unexpected or unwanted event that has caused or may cause a compromise of IT assets.
ITSG-06	A software based data sanitization method used to overwrite existing information.
ITSP.40.111	The Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Source: https://www.cse-cst.gc.ca/en/node/1831/html/26515
Job	A document processing task submitted to the hardcopy device. A single processing task may process one or more documents.
LOA3	Level of Assurance 3 – Ref: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776
Local Area Network (LAN)	Supplies networking capability to a group of computers in close proximity to each other.

Managed Print Service (MPS)	Is a service offered by an external provider to optimize or manage a company's document output. The main components provided are needs assessment, selective or general replacement of hardware, and the service, parts and supplies needed to operate the new and/or existing hardware (including existing third-party equipment if this is required by the customer). The provider also tracks how the printer, fax, copier and MFP fleet is being used, the problems, and the user's satisfaction. It is a collection of technologies, services and systems that enable improved visibility and control of the imaging environment resulting in end-user productivity and cost savings. It may include, but is not limited to, Printing Device Management components, Service Management tools and a Service Delivery Portal.
Metadata	Is data that describes other data.
MFD	Multi-Function Device
Monitoring	The continuous process of observing the operations of information systems with the objective of detecting deviations from planned or expected behaviour. Features that improve productivity, such as but not limited to: · Remotely configuring Print Devices; · Managing many Print Devices as if they were one with group-based management functions; · Checking Print Device status throughout the enterprise; · Proactively monitoring Print Device status receiving alerts on Print Device status and problems, allowing everyday issues to be resolved before users experience down-time; and · Troubleshooting problems. Features to reduce costs, such as but not limited to: · Track Print Device usage by End Users and groups to facilitate usage policies and ensure that Print Devices are deployed to provide the best fit throughout the organization. Features to help ensure security, such as but not limited to:· Centrally managing and administering critical Print Device settings to ensure consistent and correct implementation of security policies and procedures.
MPS	Managed Print Service
Multi-Function Device (MFD)	A Print Device that prints digital content onto paper, faxes digital content over a telephone line, scans paper and faxes digital content over a telephone line, and scans paper and photocopies it on paper, scan paper into digital content.
Non-digital Media	Any media that is not digitized. They are contrasted with digital media.
Non-local Maintenance	Non-local maintenance and diagnostic activities are those activities conducted by Administrators or Operators communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by Administrators or Operators physically present at the information system or information system component and not communicating across a network connection.

Operator	A person who operates the MPS and Systems. Operators may have less authority than the Administrators. An operator handles day to day needs of the system. That might involve tracking printer supplies, backup tape cartridges and other common physical elements. The system will often send messages to an operator to inform of printer problems or backup process problems for examples, and the operator is responsible for knowing how to handle the request and usually for taking any action. Messages also commonly include logical rather than physical problems. Automated processes can report problems to an operator, and the operator is responsible for knowing whatever the appropriate problem resolution procedures are for the site.
Print	A job to convert an electronic document to hardcopy form.
Print Data	The Data related to a Print Job.
Print Device	Refers to a printer (network or local), multi-functional devices, photocopiers, scanning devices and/or fax devices.
Print Job	A Print processing task submitted to the hardcopy device. A single processing task may process one or more documents.
Printer	A Print Device that prints digital content onto paper.
Protected Information	Information is "protected" if its disclosure could harm interests other than the "national interest." • There are three levels of protected information: Protected A (low-sensitive): Applies to information that, if compromised, could reasonably be expected to cause injury outside the National Interest, e.g., disclosure of exact salary figures. • Protected B (particularly sensitive): applies to information that, if compromised, could reasonably be expected to cause serious injury outside the National Interest, e.g., loss of reputation or competitive advantage. • Protected C (extremely sensitive): applies to the very limited amount of information that, if compromised, could reasonably be expected to cause extremely grave injury outside the National Interest, e.g., loss of life.
PSTN	Refers to public switched telephone network (PSTN). PSTN is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephone operators, providing infrastructure and services for public telecommunication.
Remote Access	Access to the WTD Print Solution Service Infrastructure through an external network (ex. the Internet).
Remote Management	Administrative or maintenance activities conducted by an Operator or Administrator over a network.
Risk	Refer to the definition of IT security risk.
Room	A static physical location.
RCMP	Royal Canadian Mounted Police

RBAC – Roles Based Access Control	In computer systems security, role-based access control (RBAC)[1][2] is an approach to restricting system access to authorized users. It is used by the majority of enterprises with more than 500 employees, [3] and can implement mandatory access control (MAC) or discretionary access control (DAC). RBAC is sometimes referred to as role-based security. Source: https://en.wikipedia.org/wiki/Role-based_access_control
Security Assessment	The ongoing process of evaluating the performance of IT security controls throughout the lifecycle of information systems to establish the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the departmental business needs for security. Security assessment supports authorization by providing the grounds for confidence in information system security.
Security Assessment & Authorization (SA&A)	The on-going process of evaluating the performance of IT security controls throughout the lifecycle of information systems to establish the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the departmental business needs for security. Security assessment supports authorization by providing the grounds for confidence in information system security.
Security Control	A management, operational, or technical high-level security requirement prescribed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls are implemented using various types of security solutions that include security products, security policies, security practices, and security procedures.
Security (Incident)	An unauthorized behaviour or event (against the security policy of the IT system) regarding the operation and administration of the IT system that has the potential to compromise the IT systems confidentiality, integrity, or availability.
Security Information and Event Management (SIEM)	A technology that provides real-time analysis (collection, aggregation, correlation) of security alerts generated by Infrastructure components and applications.
Security Posture	A characteristic of an information system that represents its resilience to threats, vulnerabilities, a specific set of deliberate attacks as well as accidental and natural hazards. Note: Resilience relates not only to the capability of the information system to prevent threats but also to detect, respond, and recover from their compromises.
Security Requirement	Any need, stated in a standardized language, that an information system must satisfy through IT security that contributes to achieving a business need for security.
Security Requirements Checklist (SRCL)	Personnel, facility and organisational clearance requirements.
SDP - Service Delivery Point	A Floor or a Room in a Building where the WTD Print Service or Product is implemented.
Service Delivery Portal	Means the Service Delivery Portal provided and managed by the Contractor.

Service Management Data	The data derived from the operation, administration, management of the support services and invoicing:
	a) Service Requests;
	b) Incident Tickets (excluding Security Incident Tickets);
	c) billing records and invoices at an organizational level;
	d) asset records;
	e) configuration records;
	f) system performance, capacity and resource planning information;
	g) details on devices status, error codes and events

Service Provider	An entity accountable to deliver the Service to the Clients.
SIEM	Security Information and Event Management
Site	Defined as a single floor facility or as a floor in a multi-floor facility.
Smart Card	A small electronic device about the size of a credit card that contains electronic memory and are used for a variety of purposes such as authenticating a user’s identity.
Software	An application used by an End User. Software is typically installed on Hardware.
SRCL	Security Requirements Check List
SSC	Shared Services Canada
ST&E	Security Testing and Evaluation
System	A generic term used to mean network and other devices, operating systems, computing platforms, virtualization software and applications or any combination thereof. Its use is context specific.
System Data	Any data that the Contractor uses to control or modify the operation, administration and management of the WTD Print Service which includes: a) Security Incidents; b) security information and events management (SIEM) ; c) network perimeter management (e.g. firewall); d) intrusion and prevention management; e) malware protection and security control information; f) hypervisor and virtual machine systems management; g) network management and operations; h) system configuration files, logs and scripts; i) authentication, authorization and accounting systems; j) disk systems; k) capacity and resource management systems; l) software distribution, updates and patches; and m) Directory Services.
Threat	Refer to the definition of IT threat. It refers to any potential event or act, deliberate, accidental or natural hazard, which could compromise IT assets.
Unauthorized Access	When an entity gains unauthorized access to a system. Examples include: infiltration, compromise, hacking, privilege escalation and unauthorized access/privilege.
Unauthorized Individuals	Any person who is not authorized to have access to specific systems, assets, locations, information etc.
User	An agent, either a human agent (end-user) or software agent, who uses a computer or network service.

User Data	The data related to user documents and records that are being scanned, faxed and printed as well as the associated user's account and directory data.
Vulnerability	An attribute of an IT asset or the environment in which it is located (including the security solutions) that increases the likelihood of a threat event, the probability of compromise or the severity of the outcome.
Vulnerability Assessment	A determination of the existence of information system vulnerabilities.
Wireless Network	Any type of computer network that uses wireless data connections for connecting network nodes.
Workplace Technology Devices (WTD)	A branch within Shared Services Canada. Its goal is to standardize and consolidate the procurement and provisioning of hardware and software for workplace technology devices for the Government of Canada.