COMSEC Custodian Quick Reference Guide

COMSEC Custodians are responsible for the generation, receipt, custody, distribution, safeguard, disposition or destruction, and accounting of COMSEC material entrusted to their COMSEC Account. An overview of these responsibilities follows.

COMSEC Account Management

- Ensure that other assigned duties do not interfere or conflict with your duties as a COMSEC Custodian;
- Attend a formal COMSEC Custodian training course as soon as possible following your appointment;
- Ensure that the Alternate Custodian assumes your responsibilities and duties when you are absent for a period of less than 60 days;
- Provide adequate training for Alternate Custodian(s) and Local Elements;
- Keep informed (through Information Technology [IT] Security and COMSEC publications) of any new requirements or modifications to existing equipment;
- Maintain up-to-date administrative files containing documentation related to the COMSEC Account (e.g. COMSEC Briefing Certificates, Courier Certificates, COMSEC Incident Reports and Security Screening Certificates);
- Maintain accurate and up-to-date account registration records;
- Promptly post all account registration changes to the Canadian Central Facility (CCF) Message Server or forward the changes to your Central Office of Record (COR); and
- Connect to the CCF Message Server to obtain messages on at least a weekly basis, if using Local COMSEC Management Software (LCMS).

COMSEC Accounting Reports and Files

- Ensure that accounting reports are complete, accurate and that all corrections are made in ink and initialled for paper transactions or digitally signed;
- Verify the material listed on the accounting report prior to transfer, issue, hand receipt, destruction, conversion, relief from accountability and possession;
- Return accounting reports to the originator within two working days of preparation or receipt;
- Initiate tracer action for delinquent accounting reports;
- Report any accounting discrepancies to your COR;
- Maintain accurate and up-to-date accounting files and limit access to these accounting records to authorized personnel;
- Do not apply a more stringent Accounting Legend Code (ALC), unless authorized by the National Central Office of Record (NCOR);
- Retain inactive or archive
- Mark accounting reports that do not contain classified information as “PROTECTED A (PA)”;
- Establish local accounting procedures to ensure strict control of keying material, whenever the keying material is turned over to a Temporary User; and
- Establish local accounting procedures to ensure control of COMSEC-related material such as crypto-ignition keys (CIKs), personal identification numbers (PINs), software and hardware.

Custody and Safeguard of Accountable COMSEC Material

- Store COMSEC material based on COMSEC directives;
- Maintain a record of safe combinations and limit access to the combinations to users who have a need-to-know and who possess the required security clearance;
- Ensure combinations for containers used to store COMSEC material are changed as required;
Submit requests for access to COMSEC material by foreign nationals or resident aliens to the CSEC Client Services at Communications Security Establishment Canada (CSEC);

Restrict access to keying material to the minimum number of personnel required, based on a strict “need-to-know” basis;

Immediately notify (within 24 hours) your Departmental COMSEC Authority (DCA) of any incident that may have subjected COMSEC material or sensitive information to compromise;

Mark lost or potentially compromised COMSEC material as “Pending Investigation” in your inventory file (and place the material in quarantine);

Protect the integrity of COMSEC material by:
  - inspecting the protective packaging upon initial receipt, during each inventory and prior to transfer, issue or use;
  - performing page checks on all keying material and accountable publications upon initial receipt, during each inventory and prior to transfer, issue or use;
  - promptly entering amendments to accountable publications; and
  - being able to locate every item of accountable COMSEC material held by the COMSEC Account and being aware of the general purpose for which it is being used;

Ensure that personnel who are authorized to receipt for packages containing Accountable COMSEC Material (ACM) have the appropriate secure storage (when you and your Alternate Custodian are not available);

Notify your mailroom and the personnel authorized to receipt for packages that the only ones authorized to open packages addressed to the COMSEC Account are the COMSEC Custodian and Alternate COMSEC Custodian;

Physically store effective editions of keying material, reserve editions of keying material and superseded keying material awaiting destruction in separate locations;

Store TOP SECRET keying material under two-person integrity (TPI) controls employing two different combination locks with no one person authorized access to both combinations;

Do not store COMSEC equipment in a keyed state (e.g. CIK inserted), unless operational requirements mandate it and no practical alternative exists or keyed equipment cannot be zeroized due to malfunction or damage; and

Do not remove any manufacturing labels, including the equipment nomenclature plate, the “Controlled Cryptographic Item” or “CCI” label and any other labels that identify the equipment for accounting purposes.

Distribution of Accountable COMSEC Material

Properly package, mark and ship ACM;

Obtain pre-approval from your COR for irregular or non-conventional distribution of COMSEC material;

Ensure the receiving COMSEC Account is classified or designated to the security level of the material and authorized to hold the material;

Distribute COMSEC material to Local Elements (users) who have a valid need-to-know and ensure that each user:
  - is cleared to the security level of the COMSEC material,
  - is informed of what constitutes a COMSEC incident,
  - receives a COMSEC Briefing and signs a COMSEC Briefing Certificate, and
  - understands and accepts responsibility for the protection and use of the COMSEC material;

Separate elements which, as a whole, comprise a cryptographic system (i.e. the basic cryptographic equipment, ancillaries, associated documentation and Key Variable [KVs]);

Keep individual shipments to the minimum required to support operational and contingency requirements;

List, package and dispatch keying material separately from its associated COMSEC equipment (i.e. list keying material on a separate GC-223, package separately from its associated equipment and ship in different transport vehicles);

Perform page checking and equipment checking prior to shipment;
- Send the list of effective dates of keying material separately from the keying material, on different days;
- Package Traffic Encryption Key (TEK) separately from its associated Key Encryption Key (KEK);
- Erase or zeroize KV settings in CCI equipment, components, and Common Fill Devices (CFDs) before packaging. Remove associated CKs prior to transportation;
- Identify Government Furnished Equipment as “GFE” on the accounting report and include the associated contract number. All appropriate documentation must be raised and included in the consignment or dispatched separately, if required;
- Where required, notify the receiving COMSEC Custodian of details of the shipment and estimated time of delivery;
- Initiate Tracer action if the Transfer Report Receipt (TRR) has not been received within the allotted time; and
- Immediately report (i.e. within 24 hours) the loss, improper shipment or improper handling of any COMSEC packages to your DCA. Any keying data found in place during transit (i.e. with the ECU or CFD) or upon receipt must be reported immediately to the Controlling Authority (CA), issuing COMSEC Custodian and CSEC National COMSEC Incidents Office (NCIO).

Receipt of Accountable COMSEC Material
- Notify the shipping COMSEC Account if a package has not been received within 48 hours of expected delivery;
- Carefully inspect both the inner and outer wrappings for signs of tampering;
- Immediately report (within 24 hours) any evidence of tampering to your DCA and secure the package(s) in quarantine;
- Check the contents for agreement with the enclosed Transfer Report Initiating (TRI);
- Make authorized changes to the TRR in ink and initial these changes;
  - Check that the first segment shows in any enclosed key tape canisters;
  - Complete all required publication page checks;
- Inspect the protective packaging of keying material for signs of tampering (but do not open until issued to a Local Element); and
- Never affix a label to protective packaging.

Accountable COMSEC Material Destruction
- Ensure a properly cleared and COMSEC briefed individual witnesses the destruction of all ACM;
- Use the Destruction Report as a ‘checklist’ during the destruction;
- Do not destroy COMSEC material without specific authorization;
- Ensure that personnel who perform destructions are trained in the correct procedures and methods;
- Do not destroy damaged or faulty key (submit a COMSEC incident report and return the damaged/faulty key to the National Distribution Authority [NDA] at CSEC);
- Perform equipment verification and page checking prior to destruction (normally within 48 hours);
- Destroy superseded key, whether regularly or irregularly superseded, as soon as possible after use or supersession, and do not hold longer than 72 hours following supersession;
- Destroy COMSEC publications within 15 calendar days following the date of supersession or the authorized date of destruction;
- Do not destroy COMSEC equipment, unless specifically authorized to do so;
- Ensure each segment of key is properly destroyed, and reported as destroyed, before reporting the destruction of the complete key;
- Ensure all copies of key issued to Local Elements and subordinate COMSEC Sub-accounts have been destroyed before destroying the key from which the copies were made;
- Accurately verify the material being destroyed against the Destruction Report;
- Destroy the material using approved destruction methods;
- Examine the destruction device and the surrounding area to ensure the material has been destroyed and thoroughly inspect the residue to ensure that the destruction was complete; and
- Submit Consolidated Destruction Reports containing routine destruction information to your COR on a monthly basis (no later than the 16th of the month following supersession of the key).

**Generation of Keying Material**

- Submit all requests for authorization to generate and produce cryptographic keying material to the Crypto Material Assistance Centre (CMAC) at CSEC;
- Assign ALC 6 to electronic key that will be generated from ALC 1 physical key; and
- Assign ALC 7 to electronic key that will be generated from ALC 4 physical key.

**COMSEC Inventory**

- Maintain an up-to-date inventory record of the COMSEC material charged to the COMSEC Account, including COMSEC material issued to Local Elements and COMSEC Sub-accounts;
- Limit access to inventory records to authorized personnel;
- Conduct an inventory annually upon appointment of a new COMSEC Custodian and when directed by your COR;
- Mark inventory records that do not contain classified information as “PROTECTED A (PA)”;
- Return the annual COR-initiated Inventory Report, the Amendment to Inventory Report and all supplemental accounting reports to your COR, no later than 10 working days after receipt of the Inventory Report; and
- Take corrective action to inventory discrepancies and advise your COR of the action taken, within 48 hours of receipt of the Inventory Reconciliation Status Transaction (IRST).

**Management of COMSEC Sub-Accounts**

- Establish and close COMSEC Sub-accounts, as deemed necessary, in accordance with the procedures described for opening and closing COMSEC Accounts;
- Provide formal training and interim training for COMSEC Sub-account personnel;
- Maintain a record of the inventory of all subordinate COMSEC Sub-accounts;
- Maintain a file on other associated COMSEC Sub-account information;
- Provide advice and guidance to Sub-account personnel relating to the management of their COMSEC Sub-account;
- Conduct inventory reconciliation annually with each subordinate COMSEC Sub-account;
- Audit COMSEC Sub-accounts at least every two years in order to ensure that records are accurate and control procedures are correctly applied; and
- Provide COMSEC Sub-account audit results to the National COMSEC Audit Team (NCAT) at CSEC upon request.

**In-Process Accounting**

- When applicable, maintain In-Process (IP) accounting records to ensure that appropriate IP procedures are being followed; and
- Perform a sight inventory with an appropriately cleared and briefed witness to reconcile all IP accounting records:
  - semi-annually;
  - upon the appointment of a new COMSEC Custodian; and
  - as directed by the CSEC NCAT.
COMSEC Emergency Plan

- Assist your DCA in the preparation of a plan for the protection of COMSEC material during emergencies;
- Ensure the plan clearly and concisely describes all duties;
- Inform all personnel with a need-to-know of the existence of the plan;
- Inform each individual who has duties assigned under the plan of their duties and how to carry out these duties when the plan becomes effective;
- Periodically conduct training exercises to ensure that everyone (especially new personnel) can carry out their duties; and
- Revise the plan based on the experience gained in the training exercises.