MINISTRY OF ATTORNEY GENERAL
INFORMATION TECHNOLOGY SERVICES (ITS)

ACCOUNT ACCESS FORM

******FAX ALL PAGES TO: 250 356-5210******

Questions? – Call the LOB Help Desk at 250 356-0545

☐ Create – new account ☐ Re-Create – lapsed account ☐ Delete – resigned, retired, etc. ☐ Modify – name/access change ☐ Transfer/TA – locn/Ministry change

USER DETAILS (also used to update the Global Address List)

LAST NAME | Employee # | Regular ☐ Auxiliary ☐

First Name | Initial | Title | Contractor ☐ Co-op ☐

Branch | Phone | Start Date

Division | FAX | End Date

Address | City | Postal Code

Transfer/TA from (Ministry and Branch name):

☐ Name Change – Previous Name: _____ Computer D or N # _____

MINISTRY ACCESS (only indicate access to be created, modified or deleted)

☐ E-mail ☐ IDIR (list Network shares required below) ☐ HAS IKEY Serial # _____ ☐ IKEY REQUIRED

Special Applications (include details) OR Network share drive pathname (e.g. "S12446_POCO_shr on 'OSCAR\S12446' (G:)")

Portal INTRANET Access: Group Name: _____ or NO Portal INTRANET Access ☐

☐ Spandial/VPN ☐ DTS ☐ MVS Admin Form needed

Specific Information for Access:

AUTHORIZATION

GL: Client _____ Resp. Code _____ Service Line _____ Project Code _____

X _____ Name: _____ Date: _____

(Signing Authority - NOT Applicant) (Please PRINT)

JUSTIN/CORNET Authority Signature(s): Name(s): Date:

X _____

(Not Applicant's Signature) (Please PRINT)

⇒ The authorizer is informed via e-mail once the accounts are created. Please then notify your user.
Dormant accounts of one year or more will be removed from the system.

ITSD USE ONLY

UserID | Created

IDIR | ORACLE

E-Mail | Comments

Other | Transfer requested from other Ministry (Ref #)

iKey issued / Protect File Group (CJB Users) | Notified? No ☐ Yes ☐ Date Notified

⇒ EMAIL notifications to (if NOT to Signing Authority):

CONDITIONS FOR USE OF COMPUTING FACILITY

1. As a condition of use of the BC Ministry of Attorney General facilities, and access to government computer-stored data, the user agrees not to:
   - Permit any person to use his/her username;
   - Divulge, share or compromise his/her password;
   - Use any other s username;
   - Use the facility for activities different from those for which access was granted;
   - Attempt to access or modify the data or programs of another client or user without the explicit authorization of that client or user;
   - Enable other users to access data belonging to a third party without the consent of the third party;
   - Develop or use programs, or create situations which adversely impact computer services to other clients or users;
   - Make unauthorized copies of data or proprietary software;
   - Reveal details of any checking, editing, validating, or security mechanisms, included in hardware or software, to any unauthorized persons;
   - Test or examine security related to the facility, except as provided in number 5 below;
   - Take any action, which might reasonably be construed, as injurious or detrimental to the interests of any other users or to the facility.

2. Users are responsible for all actions performed by their "usernames' except for fraudulent use of the "username" by an unauthorized third party which is not attributable in any manner to the failure of the user to properly observe the conditions for use of the computing facilities.

3. Users are required to adhere to all policies, standards or procedures pertaining to data security, naming conventions and good data processing practices. issued by the facility administrators.

4. Users of the facility should be aware that it is possible that security can be breached through causes beyond the reasonable control of the facility administrators. Users are urged to take full advantage of security mechanisms built into the systems and to change their password frequently.

5. Persons wishing to test the security of the facility, or to perform actions which may not satisfy these conditions for use, must contact *Information Technology Services* for direction as to how to obtain approval prior to conducting any tests or performing these actions;

6. The user recognizes that to monitor security, the Ministry of Attorney General, *Information Technology Services* may be required to examine data, programs, accounting, printouts, tapes, or any other data processing material used by clients or users without prior notice; and management of the computing resources will involve movement of data on disk or tape.

7. The user acknowledges that access to government computing facilities is given solely for use in the course of government business and not for personal or private communications and that all data stored on the system, including current electronic mail and information on backup tapes, are government records which can be accessed by Ministry officials in accordance with established policies and form a "record" under the *Freedom of Information and Protection of Privacy Act*

The applicant (user) agrees to:

I. Adhere to the conditions for use of the facility set out above, and

II. Advise *Information Technology Services* of the Ministry of Attorney General, or his/her Project Leader, without delay, of any circumstances, incidents or events which may impact, or are related to the privacy, availability or security of the facility or any associate computer applications.

Dormant accounts of one year or more will be removed from the system.

I CERTIFY THAT I HAVE READ AND AGREE TO THE CONDITIONS FOR USE OF COMPUTING FACILITIES:

Signature	Name	Date
X		
Applicant's Signature	Please PRINT	

12. Offender Management Systems

12.1. CORNET (revised: Feb-08)

12.1.1. Introduction

1. CORNET is the Corrections Branch electronic platform for document management, case management and quality management. It is a branch-wide information and communications tool that integrates community and custody case management data and brings document and case management to the desktop of every Corrections Branch user.
2. CORNET is designed to facilitate and enhance all elements of records entry and case management. It streamlines data entry procedures and improves data integrity through an electronic interface with JUSTIN.
3. The CORNET file is the primary location of all data relating to an inmate's involvement with the Corrections Branch.
4. CORNET is a windows-based system where users can navigate by moving between screens, pages, blocks and fields.
5. CORNET has the capacity to attach word processed or scanned documents within the Client Log.
6. This chapter describes the following areas of CORNET:
    - Access;
    - Confidentiality;
    - System security, data integrity and safeguards;
    - Security matrix;
    - Reporting system errors and enhancements; and
    - Seal/unseal youth records.
7. For detailed direction on CORNET procedures, refer to the *CORNET Users Guide*.

12.1.2. Access

Access to CORNET is provided to trained Corrections Branch employees and approved contracted staff who have been granted an individual user account. The following procedures apply:

- Users log on the system with their own user ID prior to entering or viewing data;
- CORNET tracks and maintains a footprint of user access to files; and
- Corrections Branch employees are only authorized to access Corrections Branch inmate files in CORNET when carrying out records entry, case management and administrative functions relating to the subject of the file.

12.1.3. Confidentiality

1. Corrections Branch employees are responsible to protect the privacy of clients and former clients of the branch by using the information collected only for intended and authorized purposes.
2. Users may not share, reproduce, redistribute, re-transmit, publish, transfer or exploit any information obtained from CORNET except as authorized under the *Youth Criminal Justice Act*, Youth Justice Act (B.C.), the *Freedom of Information and Protection of Privacy Act* (B.C.) and other relevant legislation and policy.
3. Employees who are in doubt as to whether certain information is confidential must ask the appropriate authority before disclosing it.
4. Caution and discretion in handling confidential information extends to disclosure made inside and outside of government and continues to apply after employment ceases.

12.1.4. System security, data integrity and safeguards

1. As a condition of use of CORNET, the user agrees not to:
    - Permit any person to use his/her username;
    - Divulge, share or compromise his/her password;
    - Use any other person's username;
    - Use the system for activities different from those for which access was granted;
    - Make unauthorized copies of data; and
    - Take any action that might be reasonably construed as injurious or detrimental to the interests of any other user or to the system.

2. CORNET is an Internet-based system that contains two databases:

    - Training; and
    - Production.

    Note: When training on CORNET, users must use the training database. Users must not use the production database when practicing on CORNET. Access to the production database will be limited to screens as designated by the user's job classification within the security matrix.

3. The System Services Unit has care and control of all data within CORNET and has the authority to edit or delete erroneous, malicious or damaging data as required to ensure the integrity and functionality of the system.
4. The System Services Unit routinely monitors the quality and integrity of data flowing into the CORNET database. When the System Services Unit is aware of recurring data entry errors from one user or correctional centre, the System Services Unit reports the problem to the assistant deputy warden, SMU, or deputy warden. The assistant deputy warden, SMU, or deputy warden ensures informal training is provided to prevent the problem from recurring.
5. In the event that data entry errors recur following informal training, the System Services Unit will contact the assistant deputy warden of SMU or deputy warden to recommend the suspension or cancellation of an individual's user access.
6. When a person who has access to CORNET is criminally charged, it may be necessary to withhold personal information from the person's Client Log if the information might put at risk a victim, third party or criminal proceeding. Correctional staff, in consultation with centre management, are authorized to maintain this personal information on the paper file. In these cases, the information can later be entered on the electronic file when it is determined that it no longer presents a potential risk.
7. Information in CORNET is subject to disclosure in accordance with the *Freedom of Information and Protection of Privacy Act*. Safety and security of the correctional centre, staff and inmates are considered before entering information that is likely to jeopardize the centre's management, operation or security.

12.1.5. Security matrix

1. CORNET contains menu tabs. Access to the information contained within each menu tab is restricted to users as defined by Adult Custody Division headquarters and designated in the Adult Custody security matrix.
2. The security matrix controls access to all menus within CORNET on three levels, depending on the user's work function and level of training:

    - User not granted access;

- User granted read-only access; and
- User granted read and write access.

3. Access to menu tabs within CORNET is determined by user work groups identified in the security matrix. Users are granted access to specific menu tabs once they have received required training.
4. The System Services Unit is the agency authorized to set up and modify user access within established work groups. CORNET user's access/modifications are completed in the following manner:
    - All CORNET access requests for new employees and approved contracted staff are submitted on the Account Access form according to the security matrix.
    - All requests to modify existing CORNET access according to the security matrix are subject to the approval of the assistant deputy warden, SMU or deputy warden.
    - All requests for user ac established work groups must be submitted by e-mail to s.15 Note: The authority confirms on the request that the appropriate level of training has been completed and includes the training attendance record and name of CORNET instructor.
    - A request for CORNET access, which is outside of the security matrix, is submitted to the Adult Custody program analyst by the assistant deputy warden, SMU, or deputy warden.
    - Within CORNET, each user is assigned a default location, which is usually the user's primary work location. While the records of each location are independent, some correctional centres are responsible for maintaining records for more than one location. When users need to access inmate records for multiple locations, they must change locations within CORNET to obtain this access.

12.1.6. Reporting of system errors, data integrity issues and enhancements

1. System errors are reported by phone during regular business hours in a timely manner to the System Services Unit by the assistant deputy warden of SMU, or deputy warden.
2. When a delay in reporting a system error outside of regular business hours could adversely impact CORNET or the operation of the centr t supervisor report the error by e-mail to the System Services Unit at s.15
3. Incidents, when data integrity is—or mised, are reported immediately by e-mail to the System Services Unit at s.15 by the assistant deputy warden, SMU, deputy warden or records supe

4. Recom em enhancements are reported by e-mail to the System Services Unit at s.15 by the assistant deputy warden, SMU, or deputy warden.

12.1.7. Seal/ unseal youth records

1. All information in the CORNET database relating to an offence committed by a person under the age of 18 or who was found guilty of an offence under the *Youth Criminal Justice Act* (YCJA) is a youth record.
2. When a record in the CORNET database meets access time limits established in section 119(2), YCJA, it is sealed. A system search performed by a user, other than authorized System Services Unit personnel, does not return sealed data.
3. Systems Services Unit personnel have authority to make available a sealed record if directed by the court. They also have authority to reactivate records when a young person has offended in other jurisdictions and access limitation periods set out in section 119(2). YCJA have not been met. If a record exists in CPIC that falls within the YCJA access periods, assistant deputy wardens, SMU, inform the Systems Services Unit.
4. A youth record includes all information collected on a young person during administration of a youth sentence. The period of access to a youth record ends as follows:
    - Extra-judicial sanctions (EJS) = two years following consent to participate in EJS;
    - Acquittal = two months after 30-day appeal period or three months following failed appeal;
    - Dismissal, withdrawal or finding of guilt with reprimand = two months following the outcome;
    - Stay = at the end of one year, if no proceedings for one year following the stay;
    - Absolute discharge = one year following finding of guilt;
    - Conditional discharge = three years following finding of guilt;
    - Summary conviction = three years after completion of youth sentence; and
    - Indictable = five years after completion of youth sentence.
5. For summary and indictable conviction offences only: When there is a subsequent guilty finding for a summary or indictable offence during the required “clean period,” an additional three or five year “clean period” is required after the end of the subsequent offence before the record can no longer be disclosed.

6. The following records are not subject to seal provisions:
    - Records regarding youth who have received an adult sentence as a result of the application of section 110(2)(a), YCJA, after the appeal period has passed or once the sentence is upheld on appeal (section 117, YCJA);
    - Records regarding youth who have received a youth sentence for a presumptive offence* (section 110(2)(b) YCJA) and the court has not ordered a publication ban (section 75, YCJA);
    - Youth records regarding adults who have been convicted of an adult offence, before the clean period for indictable and summary offences on their youth record has been satisfied (section 119(9), YCJA) are treated as adult records;
    - Presumptive offences for offenders 14 or older when charged are:
        - First degree murder;
        - Second degree murder;
        - Manslaughter;
        - Attempted murder;
        - Aggravated sexual assault; and
        - Judicially determined serious violent offences for which an adult could get more than two years in jail when Crown counsel files notice to seek an adult sentence.

12.1.8. Procedures during system outage

1. In the event of CORNET outage, users manually manage and record all functions normally performed on CORNET.
2. When CORNET is restored, users enter all information that was manually maintained during the outage.
3. Any information entered as the result of an outage must be backdated to the appropriate date and time to ensure accuracy of records.

12.2. Electronic Forms (revised: Jul-08)

12.2.1. Purpose

1. Electronic forms (eForms) provide a forms management application that addresses the needs of the Corrections Branch.
2. eForms allow users to create and manage:
    - Electronic online forms;
    - Workflow;
    - Authorizations;
    - Reports;
    - Data collection; and
    - Analysis.

12.2.2. Worklist Application

1. The Worklist Application home page permits users to:
    - Manage incoming tasks for eForms;
    - Identify eForms assigned to them or their user group; and
    - Access the eForm task details page to enter data and submit completed forms to the next level.
2. The Worklist Application home page is reviewed at least once per shift by all staff members.

12.2.3. Designation of user level

1. Creator:
    - The person assigned to initiate the primary eForm and/or the supplementary eForm is the creator of the form.
    - A creator can belong to any staffing level.
2. Reviewer:
    - The reviewer is a correctional supervisor.

3. Approver:
    - The approver is a manager.
    - The reviewer and approver cannot be the same person.

12.2.4. Reporting of system errors, data integrity issues and enhancements

1. The user reports system errors by phone to the System Services Unit at s.15 . This is done in a timely manner during regular business hours.
2. When data integrity is, or might be, c er immediately reports incidents by e-mail to the System Services Unit at s.15 or by phone.

12.2.5. Procedures during system outage

1. In the event that ICON is unavailable, users manually record all incidents on the paper version of the form.
2. When ICON is restored, users enter all information that was manually maintained during the outage.
3. Any information entered as the result of an outage must be backdated to the appropriate date and time to ensure accuracy of records.

18. CORNET Policy

18.1 Overview (revised: Dec-06)

18.1.1 Introduction

1. CORNET is the Corrections Branch electronic platform for document management, case management and quality management. It is a branch-wide information and communications tool that integrates community and custody case management data. It brings document and case management to the desktop of every Corrections Branch user.

2. CORNET is designed to facilitate and enhance all elements of case management. It streamlines data entry procedures and improves data integrity through an electronic interface with JUSTIN.

3. As a result of improved functionality, CORNET enables a realignment of certain responsibilities between probation officers and administrative staff in Community Corrections offices.

4. This chapter describes in detail the three areas of CORNET functionality: slate management, case management and quality management.

5. For direction on CORNET procedures, refer to the *CORNET Users Guide*.

18.1.2 CORNET Access

Access to CORNET is provided to Corrections Branch employees who have an individual user account. The following procedures apply:

- Users log on the system with their own user ID prior to entering or viewing data;
- CORNET tracks and maintains a footprint of user access to files; and
- Corrections Branch employees are only authorized to access Corrections Branch client files in CORNET when carrying out case management and administrative functions related to the file subject.

18.1.3 Case management tools

1. The CORNET file is the primary location of all data related to a client's involvement with the Corrections Branch.

2. Case management is conducted and recorded in CORNET using the tools set out in this section:

    - Client logs—integrated community and custody running records with the capacity to attach word-processed documents;
    - Event-triggered automated log entries;
    - Notifications to case managers of new information, program wait-lists, external referrals, and viewable documents;
    - Cross-linking of information in the system to orders and order expiries; and
    - Flexible rules that allow data entry by staff in locations other than where the client is currently active.

18.1.4 Client log

1. The Client Log replaces community running records.
2. All case recording notes are entered in the Client Log.
3. Users can enter concise detailed information about regular client contact or attach formatted documents such as initial entries and summaries.
4. Users can enter a record on the Client Log for clients who are inactive in the community or active with another probation officer/ probation officer 14.
5. Probation officer/ probation officer 14 responsibilities:

    - Records initial entry, case management plan;
    - Records results of contacts with a client and related case management information, including assessment results and collateral information;
    - Makes entries in the Client Log regardless of whether the client is assigned to the PO/PO14;
    - Attaches interim summaries, including an updated case management plan every six months or more frequently as deemed necessary by the primary case manager;
    - Attaches a transfer summary before an inter/intra office transfer of file;
    - Attaches a termination summary upon conclusion of supervision;

- Attaches pre-sentence reports, technical suitability reports and community assessments to the Client Log following disposition or decision; and
- Scans or attaches correspondence to the Client Log.

18.1.5 Information in CORNET—Client Log

Refer to subsections 8.3.1, Case recording standards, and 8.3.2, Information recorded in CORNET, for guidance on Client Log contents.

18.1.6 Client paper file content

1. The permanent client physical file contains the following items:
    - Client information screens printouts:
        - Client Profile;
        - Addresses and Communication Devices; and
        - Client Physical Description.
    - Court documents;
    - Breach reports;
    - External documents that do not exist in CORNET and cannot be attached;
    - Appointment slips;
    - Most recent summaries printed from the Client Log (interim, transfers); and
    - Temporary PSR and TSR notes remain on the file until the end of an appeal application, during an appeal or upon completion of an appeal. Notes that issues about addresses important to case management are transcribed into the Client Log if they contain information not included in the report.
2. Files that are active, re-opened or created as of February 7, 2005 must meet the above requirements. File contents existing prior to February 7, 2005 can be maintained in accordance with requirements prior to this date.

18.2 Slate (Document) Management (revised: Mar-11)

18.2.1 Document management—court offices

1. Documents in CORNET are managed using slates. Slates are screens that contain lists of items that can be scrolled through, sorted and printed.

2. This section addresses responsibilities regarding slate management.

18.2.2 Slate management

1. CORNET automatically fills in certain information depending on the user. Because courts can make changes to a document at any time (manually or in JUSTIN), the user transfers a document into CORNET only after obtaining a signed paper copy.

2. Before assigning the CS# or creating a participant link, the user views conditions of the order to ensure that it contains a reporting condition.

3. An order is considered to be on the system when it appears on the JUSTIN Documents slate. Users check the JUSTIN Documents screen from the Document Summary screen when looking for active orders.

4. A probation officer/ probation officer 14 may perform some responsibilities identified as administrative staff functions.

18.2.3 Administrative staff slate maintenance and related responsibilities

1. Manage the Pending Arrivals slate.

2. Transfer orders from JUSTIN Documents screen into CORNET.

3. Admit, assign, transfer and code both JUSTIN documents and incoming referrals.

4. Clear Pending Arrivals slates of non-reporting orders on a daily basis:*

    - Create a participant link between CORNET and JUSTIN, as required;

    - Refer clients to another office, as required; and

    - Print reports from the Report Parameters screen, as required.

* Note: Despite the absence of a reporting condition, before clearing the slate, ensure that the order does not have other optional conditions that indicate Community Corrections responsibility. When a responsibility is indicated, admit or refer.

18.2.4 Pending Arrivals and JUSTIN Documents slates (when a client reports)

1. Administrative staff responsibilities:

    - Initiate a search if client is not linked to JUSTIN (i.e. if no CS# fills the slate);
    - Locate client in CORNET and view photo on Client Profile to confirm ID;
    - If no photo exists, view identification to confirm ID and photocopy;
    - If client does not exist in CORNET, assign new CS#;
    - If no link has been created between CORNET and JUSTIN, create a participant link;
    - Confirm address and manually enter or transfer it from JUSTIN;
    - Admit client to location, assign client to primary case manager or select referral type, refer client/report to appropriate office, giving two days to report;
    - Assign client to primary case manager for report preparation; and
    - Transfer and code all documents not being referred.

2. Probation officer/ probation officer 14 responsibilities:

    - If client is referred:
        - Review referral and make necessary changes;
        - Give client verbal direction to report; and
        - Sign referral with client.
    - If client is admitted, PO/PO14 completes/updates the remaining admit screens. When directed by the local manager, administrative staff assist with entry of the admit screens in CORNET. They may also assist with client photos if such photos can be taken from within a secure area:
        - Client Names;
        - Client Physical Description;
        - Maintain Client Photo;
        - Client Alerts;

- Addresses and Communication Devices;
- Client Visitor / Contact / No Contact (enter victims and contact person);
- Client Characteristics and Identifiers; and
- Print client ID card.

3. Initial entry on Client Log screen is completed.

18.2.5 Pending Arrivals and JUSTIN Documents slates (when a client does not report)—administrative staff responsibilities

No later than two working days, following the scheduled reporting time:

1. Refer—if client is active to another office, complete a document-only referral to client's active location.
2. View and transfer document—if client is active at current location or to create a pending relationship to current location, transfer and code the order.
3. If client is new, assign supervision to a probation officer/ probation officer 14.

18.2.6 Incoming referrals for non-court offices (when a client reports)

1. Incoming referrals are already linked to JUSTIN and have a CS# attached (participant link).
2. Administrative staff monitor Pending Arrivals slate and notify appropriate probation officer/ probation officer 14 when action is required.
3. Administrative staff responsibilities:
   - Confirm address and manually enter or transfer it from JUSTIN into CORNET;
   - Admit client to location, assign client to primary case manager or select referral type; and
   - Transfer and code all documents not being referred.
4. Upon completion of steps 1 to 3, the probation officer/ probation officer 14 assumes responsibility for completion of intake procedures and reviews and/or completes the procedures set out in 18.2.4(2).

18.2.7 Incoming referrals for non-court offices (when a client does not report)—PO/PO14 responsibilities:

1. Incoming referrals are managed on the Pending Arrivals slate no later than two working days following scheduled reporting time.

2. Probation officer/ probation officer 14 responsibilities:

    - Confirms that the client has not reported and changes status of the referral from "open" to "failure to report"; and

    - Transfers and codes the order if the client is already active to a primary case manager.

18.2.8 Referrals from institutions

1. When a client has active or future orders at a community location, the institution issues an RTC referral to the community location when the client is released from custody. Referrals are completed on new orders and continuation of existing orders.

2. CORNET automatically closes the referral when the community office admits the client.

3. For clients already supervised by a community location, the community location manually closes the referral by changing the status to *complete* once the client reports.

4. The CORNET default may result in an inmate being directed to report to an itinerant office. When this occurs, the PO/PO14 initiates contact with the correctional centre prior to the inmate's release and provides written directions for the inmate to report to the itinerant office. Correctional centre staff have the inmate sign the written instructions acknowledging the direction to report, and complete the referral to community entry on CORNET.

18.2.9 Varied orders—administrative staff responsibilities

1. Locate varied orders on the Pending Arrivals slate.

2. Determine if document contains new direction to report to the default court location.

3. If there is no new reporting condition and client is active to the current location, notify supervising probation officer/ probation officer 14.

4. If there is no new reporting condition and client is active to another office, create a referral without reporting direction to the active office.

5. If there is a new reporting condition directing client to report to the court default office, the document is treated as a regular JUSTIN document.

18.2.10 Varied orders—PO/PO14 responsibilities

1. Upon being informed of an order variation (via Notification slate or administrative staff).

2. Primary case manager locates client's varied order on the JUSTIN Document slate, views the variation and attributes it to the appropriate document.

3. Deletes varied order from JUSTIN Documents slate.

18.2.11 Judicial Justice Centre default court office

1. The Judicial Justice Centre (JJC) is a centralized location that conducts afterhours bail hearings for the entire province.

2. When a court file number already exists in JUSTIN, the JJC produces electronic documents in JUSTIN and distributes them electronically to the JUSTIN Document Slate of the default court probation office where the next court appearance is scheduled.

3. When a court file number does not already exist in JUSTIN, the JJC produces documents via the intranet and distributes them by fax to the court registry where the person will be making their next appearance. The receiving court registry is then responsible for scanning the documents and distributing them to the JUSTIN Documents Slate of the default court probation office where the next court appearance is scheduled.

18.2.12 CORNET client physical file

1. The Client Physical File screen is used to track community and custody files for individual clients. It contains information about the creation, sending, and receiving of client files. When there is no existing file, the system automatically creates a file record upon admission of the client, assignment of a report or creation of a pending relationship.

2. If no adult community corrections file exists, administrative staff create a physical file when:

    - A client is admitted;

    - An order is entered to create a pending relationship; and

    - A report is assigned.

3. Administrative staff create a record on the Client Physical File screen when a file is:

    - Sent to another location;
    - Received at their location;
    - Sent to off-site storage; and
    - Received from off-site storage.

4. Record on the Client Physical File screen the following events:

    - Send event—prior to a client file being mailed to another office;
    - Received event—when a client file is physically received; and
    - Off-site storage—prior to sending inactive files to off-site storage, record accession number and earliest destruction date.

18.2.13 Reports—introduction

1. The Client Report Details screen allows the user to enter and view information about major and minor reports for a specific client.
2. The user can enter a close date for the report and indicate whether it was completed.
3. The report and assignment details are entered when the report request is transferred from the Pending Arrivals and JUSTIN Documents slates.
4. Breach Reports to Crown Counsel automatically update with Crown's decision.

18.2.14 Reports— probation officer/ probation officer 14 responsibilities

1. Major reports (ADR, PBR, TAR, ADR, PSR, TSR, CSR, FST, HCR, ATP, PDR, PSR, ASS):

    - Ensure report details are correct;
    - Enter report close date;
    - Indicate whether report was completed; and
    - If report was not completed, enter reason.

2. Minor reports (ABB, ABR, BCS, 733, 811, MCS, PSS, PTH):

    - Enter report details;
    - Enter report close date; and
    - Indicate that report was completed.

18.2.15 Report requests

1. Report requests appear on the Pending Arrivals slate and JUSTIN Documents slate. The default court probation office can refer the report request to another office or accept it at that location.

2. Administrative staff are responsible for checking the Pending Arrivals screen daily to monitor report requests. They assign them as required by the local manager within one working day.

    Note: Pre-sentence report requests from court of appeal and requests for progress reports do not show on the Pending Arrivals screen because they are not in JUSTIN.

3. Default office administrative staff responsibilities:

    - Confirm that office/officer will complete report, if subject is under supervision;
    - Refer report request to appropriate office based on address;
    - Indicate on report referral if reporting direction was given; and
    - Forward package, including court request and police report, when received.

4. Receiving office administrative staff responsibilities

    - View and transfer report request into CORNET;
    - Assign report to probation officer/ probation officer 14 on Client Reports screen; and
    - Enter completion details on Client Reports screen.

18.2.16 Community assessments

1. Within two working days of receiving the request for a community assessment entered by the custody centre, the primary office enters the information into the CORNET Client Reports screen.

2. The office completing the report indicates on the CORNET Client Reports screen whether the report was completed or not completed.

18.3 Case Management (revised: Aug-09)

18.3.1 Probation officers / PO 14s responsibilities

1. Complete required RNAs on RNA Forms screen.
2. Refer clients to programs on Client Program Summary screen.
3. Maintain client log entries on Client Log screen.
4. Monitor and manage Notification slate on a daily basis.
5. Update critical dates for six-month review by reviewing Notification slate.
6. Record actions taken in response to notifications on the Client Log screen.
7. Enter major reports completed.
8. Enter breach reports on Client Reports screen once completed in JUSTIN.
9. Complete transfer referrals for active clients from Referral Summary screen.
10. Administratively close or re-open a client's file on the Administrative Close screen, as required.
11. Manually release clients on Client Release screen when clients are released prior to natural expiry date of their last active order.
12. Maintain a current contact person on Visitors/ Contacts/ No Contacts screen.
13. Maintain current record of conditional sentence order incidents on the CSO Calculation screen—incidents are recorded within two days.
14. Print reports from the Report Parameters screen as required.
15. Enter victim information.
16. Maintain current Address and Communication Devices.
17. Primary case manager is responsible for entering the secondary case manager on the Client Supervision Assignment screen.

18.3.2 Notification slate

1. The Notification slate displays information about certain events or dates that are relevant to the management of clients on a user's caseload. Certain notifications can be acknowledged directly on the slate and an entry made in the Client Log. Other notifications require the user to complete a task elsewhere in the system.

2. Probation officer/ probation officer 14 responsibilities:

    - Check their Notification slate at least once per day to monitor and acknowledge relevant notifications;

    - Manage notifications within two working days of the notification date;

    - Notifications that cannot be managed within two working days are brought forward ("BF'd") with an explanatory note in the Client Log; and

    - Primary case manager informs secondary case manager of relevant notifications and makes a note in the Client Log that secondary case manager was informed;

18.3.3 Victim information on CORNET

The following section outlines screens used by Corrections Branch staff when recording victim information.

1. Client Visitors/ Contacts/ No Contacts screen:

    - If the victim is a court-ordered no-contact, the primary case manager enters only the name on this screen.

2. Victim List screen:

    - Summarizes information entered on each victim. PO/PO14s enter new victims or view information.

3. Victim Details screen:

    - The primary case manager enters the victim's name, address, and telephone number.

4. Victim Contact Log:

    - The primary case manager enters details of all communications with the victim in the Victim Contact Log.

5. Client Log:

    - The primary case manager references contact with a victim in the Client Log. Particulars of the victim contact and identifying details are entered on the Victim Contact Log. Client log does not contain information that could lead to identifying the location of the victim.

18.3.4 Risk/needs assessments

1. The Notification slate alerts the probation officer/ probation officer 14 to the requirement for an assessment or reassessment.

2. The notification is removed from the slate when the assessment is completed.

3. PO/PO14s enter a note in the Client Log listing the documents reviewed and collateral contacts made for the assessment, and indicating when the assessment was complete.

18.3.5 Core programs—introduction

1. CORNET allows core program facilitators to define the schedule of core programs that are available at their location.

2. Probation officers can look at programs offered at all locations and place a client on the wait-list.

3. CORNET records a history of programming details for each client and indicates full, partial or non-completion.

18.3.6 Core programs—facilitator responsibilities

1. Creates a schedule and indicates which programs are available at their location. When directed by the local manager, administrative staff assist with data entry of the program schedule in CORNET.

2. Indicates who is facilitating core programs.

3. Enrols clients from the wait-list into the program.

4. Indicates with a comment the reason(s) a client was not accepted into the program.

5. Records weekly attendance and participation comments for each enrolled client on the Program Attendance and Outcome screen.

6. Upon completion of the core program, records outcome for each enrolled client.

7. If required, makes recommendations on the Program Attendance and Outcome screen.

18.3.7 Core programs—probation officer/ probation officer 14 responsibilities

1. Refers clients to core programs via the Client Program Summary screen.

2. Clients can only be referred to programs at offices other than the supervising office when there is an agreement to accept out-of-office referrals between local managers of the referring and receiving offices.

18.3.8 Conditional sentence calculation—introduction

1. The Conditional Sentence Calculation screen allows the user to maintain a chronological history of events as it pertains to a particular conditional sentence.

2. Users select incidents from a list of values and attribute them to the CSO calculation.

3. Some events stop the clock from running (e.g. time is not counting down on the order). Other incidents start the clock again.

18.3.9 Conditional sentence calculation—general principles

1. A separate conditional sentence order (CSO) calculation is required for every CSO that runs individually.

2. In addition to being a method of calculating days remaining, the CSO Calculation screen is a history of events that relates to the CSO.

3. Community Corrections is responsible for maintaining CSO calculations until the judge directs that the order is terminated.

4. Upon termination of the order, the calculation becomes the responsibility of the institution.

5. Institutions refer to the community calculation as a point of reference when completing the institution calculation upon termination of the CSO.

6. Institutions are responsible for verifying community calculations before relying on them.

18.3.10 Conditional sentence calculation —probation officer/ probation officer 14 responsibilities

1. Enter incidents into the CSO Calculation screen within two working days of occurrence.
2. Enter relevant incidents on the CSO Calculation screen regardless of whether they affect the running of the clock or final calculation.
3. Recalculate to accurately determine number of days remaining.
4. Monitor the Notification slate to manage information that relates to CSO calculation.

18.3.11 Conditional sentence calculation—local manager responsibilities

The local manager reviews all conditional sentence order (CSO) cases when a breach of a CSO is filed and either withdrawn or resolved by the court, or a new sentence is imposed by the court.

18.3.12 External program—PO/PO14 responsibilities

1. The External Program screen allows the user to record referral and outcome information for programs run by external agencies.
2. A probation officer/ probation officer 14 records:
    - Referral details for external programs on the External Program screen;
    - Comment indicating the reason(s), if subject is not accepted into the program;
    - Start date on External Program screen at start of the program;
    - Program end date on External Program screen at the end of the program;
    - Client's outcome at the end of the program; and
    - Recommendations made by external program facilitator.

18.3.13 Release to parole from a provincial custody centre

1. The Notification slate alerts the probation officer when a client is released from provincial custody to parole. The notification identifies the federal parole office that will provide supervision and prompts the probation officer to administratively close any pending orders to "Federal Parole" in CORNET.

2. The administrative close procedure in CORNET prevents pending orders from becoming active before parole expiry has been confirmed with the federal parole office.

3. The Notification slate alerts the probation officer seven days prior to the final warrant expiry date of parole. This notification prompts the probation officer to contact the federal parole officer to arrange transfer of supervision to Community Corrections.

4. The probation officer manually reverses the administrative close procedure in CORNET when the client reports to Community Corrections.

18.3.14 Seal/unseal youth records

1. All information in the CORNET database, related to an offence committed by a person under the age of 18 or who was found guilty of an offence under the *Youth Criminal Justice Act* (YCJA), is a youth record.

2. When a record in the CORNET database meets access time limits established in section 119 (2) YCJA, it is sealed. A system search performed by a user, other than authorized System Services Unit personnel, does not return sealed data.

3. When accessing the Client History, the probation officer/ probation officer 14 verifies that the information complies with the *Youth Criminal Justice Act* access time limitations (set out below) prior to applying the results for assessment or report purposes. If discrepancies are noted, the PO/PO14 reports the concern to Systems Services Unit and a program analyst via e-mail.

4. Systems Services personnel have authority to make available a sealed record if directed by the court. They also have authority to reactivate records when a young person offends in other jurisdictions and access limitation periods set out in section 119 (2) YCJA are not been met. If a record exists in CPIC that falls within the YCJA access periods, PO/PO14s inform the Systems Services Unit.

5. A youth record includes all information collected on a young person during administration of a youth sentence. The period of access to a youth record ends as follows:

    - Extrajudicial sanctions (EJS): Two years following consent to participate in EJS;

    - Acquittal: Two months after 30-day appeal period or three months following failed appeal;

    - Dismissal, withdrawal or finding of guilt with reprimand: Two months following the outcome;

    - Stay: At the end of one year, if no proceedings for one year following the stay;

- Absolute discharge: One year following finding of guilt;
- Conditional discharge: Three years following finding of guilt;
- Summary conviction: Three years after completion of youth sentence;
- Indictable: Five years after completion of youth sentence;
- For summary and indictable conviction offences(when there is a subsequent guilty finding for a summary or indictable offence during the access period): An additional three or five-year access period is required after the end of the subsequent offence before the record can no longer be disclosed.

6. The following records are not subject to seal provisions:

- Records regarding youth who receive an adult sentence as a result of the application of section 110 (2) (a) YCJA, after the appeal period or when the sentence is upheld on appeal (section 117 YCJA);
- Records regarding youth who receive a youth sentence for a presumptive offence* (section 110(2) (b) YCJA) and the court does not order a publication ban (section 75 YCJA);
- Youth records regarding adults who are convicted of an adult offence (excluding provincial statute offences and absolute/conditional discharges), before the access period for indictable and summary offences on their youth record is satisfied (section 119(9) YCJA), are treated as adult records;

* Presumptive offences for offenders 14 or older when charged are:

  - First-degree murder;
  - Second-degree murder;
  - Manslaughter;
  - Attempted murder;
  - Aggravated sexual assault; and
  - Judicially determined serious violent offences for which an adult could get more than two years in jail when Crown counsel files a notice to seek an adult sentence.

16. Information Systems

16.1 Objectives

1. Maximize the effectiveness and efficiency of Branch services through management of information systems.

2. Provide secure, efficient and reliable methods of entering, recording, and reporting information about Branch activities, including programs, clients, personnel and resources.

3. Provide the public, government, Branch, and other justice agencies with accurate and timely information for operations, management and research.

4. Provide opportunities for staff at all levels to learn relevant systems and apply their skills in the workplace.

5. Facilitate exchange of information within the Branch, and between the Branch and other parties within and outside the Ministry.

6. Maintain the business rules of systems to reflect current policy and procedures, legislative changes and responses to case law.

7. Ensure the systems reflect current technological standards, including security and database design.

16.2 Systems Security

16.2.1 Treatment of data

1. Corrections Branch information systems contain current and historical data related to activities of Branch clients and contracted agencies.

2. The security, integrity and accuracy of this data is essential to:

    - Protect public safety;
    - Safeguard adherence to court orders;
    - Support management decisions;
    - Account for financial transactions; and
    - Provide accurate data to other Branch or Ministry systems.

16.2.2 Ensuring data integrity

1. Systems information must accurately reflect information contained in original court documents.

2. Client information must be accurately maintained throughout active Branch involvement and adhere to rules and principles of the Freedom of Information and Protection of Privacy Act (FOIPPA).

3. Upon receipt, all orders, warrants and significant events—such as escapes—must be entered no later than the end of the next working day.

4. The last service delivery or off-site storage location for community and institutional manual files must be recorded in CORNET.

16.2.3 Measures to protect access

1. *Unique user identification and passwords*: All systems require users to change their passwords after a period of time, and do not allow users to re-use passwords. Every user submits an access request form stating their position, names of systems they need to access, and the signature of the approving supervisor. This form outlines the roles and responsibilities of users, and confirms that they meet legal or regulatory requirements. User IDs and passwords are unique for each individual user, and passwords must not be shared.

2. *Log-out*: Users are automatically logged out of the system after inactivity.

3. *Graduated levels of user access*: Access is based on the user's "need to know," and training.

4. *Audit trails*: Entries, amendments, and/or deletions of key fields are dated and identify the staff member making the entry, amendment and/or deletion. Branch information systems are subject to operational audit by the Investigation, Inspection and Standards Office.

5. *Confidentiality agreements*: Contracted staff who work on systems maintenance or development are required to sign confidentiality agreements regarding Branch data.

6. *Electronic Access Agreements* (EAA) *for external users*: Electronic access to Branch information by external users is supported by an EAA. EAAs use the Ministry template and guidelines.

16.2.4 Systems policy and training

1. *Corrections Branch Systems Policy and Training Steering Committee*:

   The Steering Committee is responsible for:

   - Overseeing development of systems policy and a training model;
   - Ensuring resources are provided for trainers and the development of policy/reference/training manuals; and
   - Providing classrooms for regional systems training.

2. *Steering Committee membership*: At a minimum, membership includes one senior representative from each division of the Branch, the Justice Institute of B.C., and the Manager, Information Technology, Systems Services Unit. The Provincial Director, Strategic Planning and Corporate Programs Division, chairs the committee.

3. *Working Group*: The Steering Committee appoints members to the Systems Policy and Training Working Group to advise the Steering Committee. It also implements initiatives related to systems policy and training.

4. *Training certification of users*: Access to a system is granted only to Branch personnel who have completed the required level of training that:

    - Is based on the user's "need to know" or current job description;
    - Conforms to provincial curriculum standards; and
    - Is taught by certified trainers.

5. *Competency testing:* Competency must be demonstrated by users prior to being granted system access.

6. *Responsibility of Systems Services Unit:* The Manager, Information Technology, Systems Services Unit is authorized and responsible for:

    - Certifying systems trainers; and
    - Approving provincial curriculum standards and materials used in systems training.

16.2.5 Misuse of information systems

1. Misuse of Branch systems is investigated when anyone:

    - Gains unauthorized access or provides others with unauthorized access to systems, networks, servers, applications, databases, personal computers, digital files, and other information or security technologies controlled by the Corrections Branch;
    - Uses Branch systems for unauthorized or commercial purposes;
    - Provides systems data or information about the system to unauthorized persons, agencies or organizations; or
    - Alters, adds or deletes systems data without authorization.

2. Unauthorized use of electronic access may result in suspension or termination of access. Access may be re-approved when the authorizing manager or designate is satisfied that the circumstances of the unauthorized use have been addressed.

3. The Manager, Information Technology, Systems Services Unit has authority to temporarily suspend access to individual users who are suspected of misusing information systems. The Manager, Information Technology is responsible for investigating suspected misuse and reporting to the Assistant Deputy Minister. Only the Assistant Deputy Minister has authority to direct that access to an individual user or an external user group be terminated.

4. Electronic Access Agreements identify potential consequences of unauthorized use of electronic access. Access is denied unless the user signs an acknowledgment of their responsibilities.

16.3 Information Systems Authorization and Training

16.3.1 Responsibility for authorization

1. Authorization may only be granted by delegated personnel to access a system, network, server, application, database, personal computer, terminal, printer, digital file, and information or security technology controlled by the Corrections Branch.

2. In general, Provincial Directors, District/ Local Directors, and Regional/ Local Managers or their designates acts as authorizing personnel. Access levels are based on job functions of users and their "need to know."

3. Authorizing personnel are responsible for requesting removal or modification of access levels to Branch systems, if the job functions change, the staff member resigns, or employment is terminated.