

---

# PART E OPERATIONAL DOCUMENTS

---

## CONTENTS

- [1.0 Electronic Access to JUSTIN Information and Application Package](#)
- [2.0 JACS Committee Evaluation Guide for Applications for Electronic Access](#)
- [3.0 Form Letters](#)
- [4.0 Memos](#)
- [5.0 JUSTIN Public Inquiry Terminal Use Notice](#)
- [6.0 Account Access Form](#)

## 1.0 Electronic Access to JUSTIN Information and Application Package

To obtain a copy of this Information and Application Package to in order to apply for electronic access, please send an email request to:  
[AGCSBJACSCCommittee@gov.bc.ca](mailto:AGCSBJACSCCommittee@gov.bc.ca)



**ELECTRONIC ACCESS  
TO INFORMATION IN JUSTIN  
INFORMATION AND APPLICATION  
PACKAGE**

**JUSTIN Access and Security Committee**

## IMPORTANT – PLEASE READ BEFORE USING THIS PACKAGE

This package is designed for organizations that request electronic access to the Justice Information System (JUSTIN), which is B.C.'s operational integrated criminal case management system and the electronic court record.

Electronic access to JUSTIN means ongoing, direct access to the JUSTIN application and database, where the party receiving access has an ongoing operational requirement for access to information in JUSTIN.

Electronic access to JUSTIN is governed by the JUSTIN Electronic Access Policy, which is administered by the JUSTIN Access and Security Committee (JACS Committee). In order to obtain electronic access to JUSTIN, an organization must do the following:

1. Complete the application form contained in Part F of this package, submit it to the JACS Committee, and demonstrate that the access requested satisfies the criteria for electronic access to JUSTIN outlined in Part D of this package.
2. Meet any technical or security specifications required to ensure that the requested access is feasible and does not present an unacceptable risk to the information in JUSTIN.
3. Sign an electronic access agreement stipulating the terms and conditions of access.
4. Have all of its personnel requiring access to JUSTIN undergo a security clearance prior to receiving access to JUSTIN. At a minimum, this security clearance will require a name check for a criminal record, and might also include a fingerprint or other background check depending upon the information to be accessed.
5. Pay some or all of the costs associated with establishing and supporting the access. These might include training, network costs, upgrades to software or hardware, or other systems changes.

This application package is only for applicants who wish ongoing, direct electronic access to the JUSTIN application and database. If your organization does not require ongoing operational access to information in JUSTIN, you should not use this application package. Instead, please send a letter as an e-mail attachment outlining the information required in as much detail as possible to:

Chair, JUSTIN Access and Security Committee

Court Services Branch Headquarters

[AGCSBJACSCCommittee@gov.bc.ca](mailto:AGCSBJACSCCommittee@gov.bc.ca)

Phone: (250) 356-1548

Fax: (250) 356-8152

## Introduction

---

Electronic access to the information in JUSTIN may be permitted where providing access is consistent with the fundamental purposes of JUSTIN and any applicable law and policy. To this end, the JUSTIN Access and Security Committee (JACS Committee) has developed comprehensive policy that includes criteria for permitting access to JUSTIN.

This Information and Application Package is intended to provide potential applicants for electronic access to JUSTIN with information about the requirements related to applying for electronic access.

## Using this Document

---

This document is divided into 6 parts:

- Part A provides background information on JUSTIN.
- Part B provides answers to frequently asked questions about access to information in JUSTIN.
- Part C lists the technical requirements for obtaining electronic access to JUSTIN.
- Part D outlines the JUSTIN Electronic Access Policy provisions on allowing electronic access to JUSTIN.
- Part E contains a flowchart showing an overview of the application process.
- Part F contains the application form for electronic access to JUSTIN.

## **PART A: Background**

### **What is JUSTIN?**

---

The Justice Information System (JUSTIN) is an operational integrated criminal case management system and the electronic court record. It is the provincial repository of information about all adult and youth criminal cases arising in the province, from initiation through to disposition. JUSTIN also contains information about offences pursuant to provincial legislation and is used by the Provincial Court for criminal and civil trial scheduling.

### **What information is in JUSTIN?**

---

JUSTIN is the provincial repository of information about all adult and youth criminal cases arising in the province, from initiation through to disposition and the electronic court record. JUSTIN also contains information about offences pursuant to provincial legislation. Information in JUSTIN includes the name of an accused or convicted offender, the charge, the status of a court proceeding and the final outcome of a court proceeding.

### **Why was JUSTIN developed?**

---

JUSTIN was developed for use by criminal justice agencies and the Judiciary for public safety purposes, law enforcement purposes, and the effective and efficient administration of the criminal justice system. JUSTIN was also developed for use by the Provincial Court for criminal and civil trial scheduling. Through JUSTIN, information is shared and re-used by police, Crown counsel, court registries, Judicial case managers, corrections personnel and other justice agencies.

## How is JUSTIN organized?

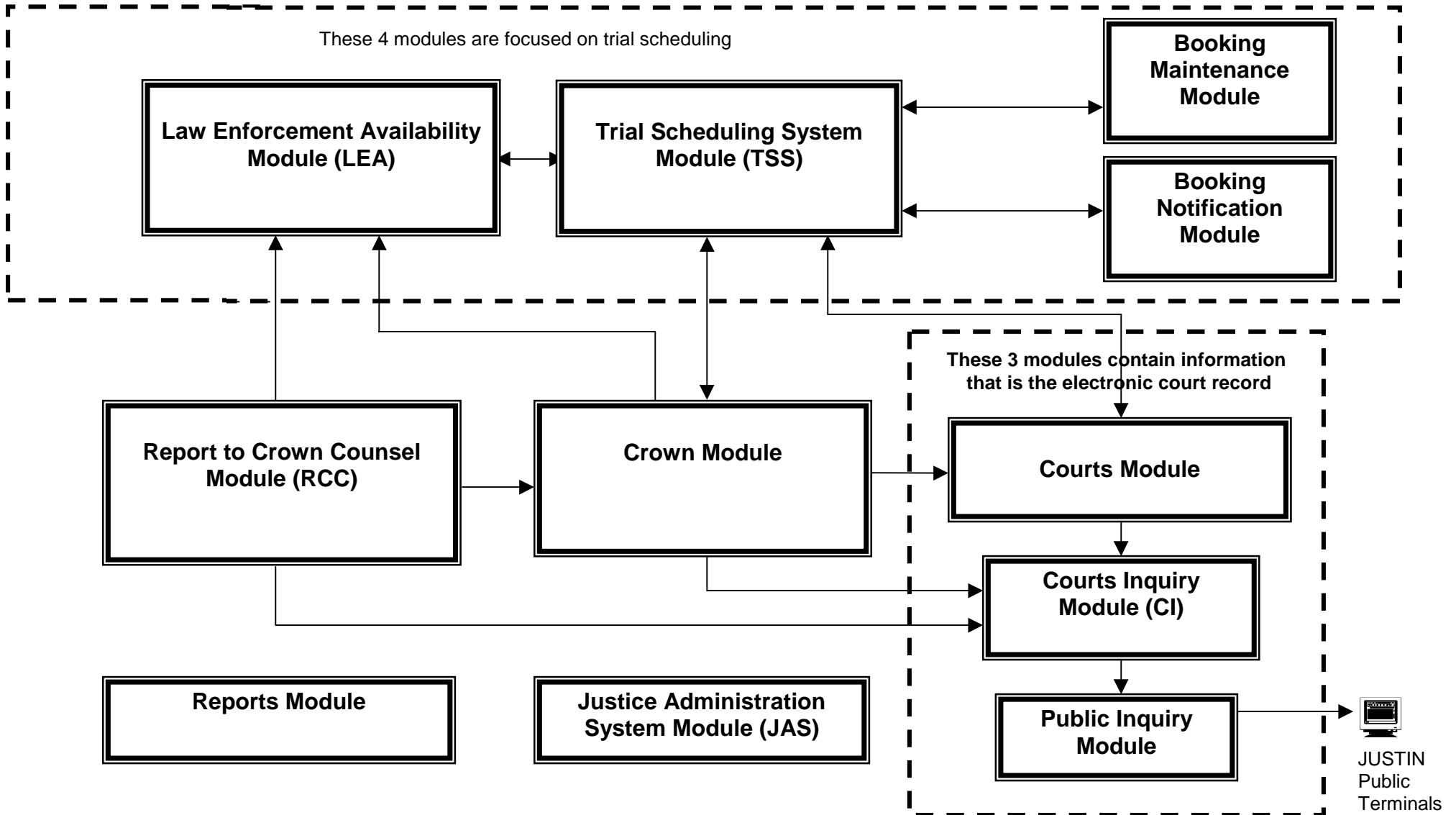
JUSTIN is comprised of modules that allow authorized users to view specified information in JUSTIN. The name of each module and its basic functionality is outlined in Figure 1. An illustration of the JUSTIN modules within the JUSTIN application is shown in Figure 2.

*Figure 1 – Description of JUSTIN Modules*

<b>MODULE</b>	<b>DESCRIPTION</b>	<b>USED BY</b>
Report to Crown Counsel (RCC) Module	The RCC module is used to submit and process Reports to Crown Counsel. Electronic access to the RCC Module automatically provides electronic access to the Courts Inquiry Module.	Municipal police, RCMP, and other law enforcement agencies
Crown Module	The Crown Module is used to prepare charge assessments and produce Informations and Indictments, which can then be forwarded electronically to Court staff.  Electronic access to the Crown Module automatically provides electronic access to the Courts Inquiry Module.	Federal and Provincial Crown counsel
Courts Module	The Courts Module is the electronic court record. It is used for case management and case tracking. It records information about the accused, charges, court appearances, documents, and results. It includes non-public information about pardoned convictions and about cases with publication or disclosure bans.  Electronic access to the Courts Module automatically provides electronic access to the Courts Inquiry Module.	Court Services Branch staff
Courts Inquiry Module	The Courts Inquiry Module is used to search specific cases for information about court	Courts Services Branch staff, criminal justice

<b>MODULE</b>	<b>DESCRIPTION</b>	<b>USED BY</b>
	appearances and case results. It includes non-public information about pardoned convictions and about cases with publication or disclosure bans.	agencies, law enforcement agencies
(Courts) Public Inquiry Module	The Public Inquiry Module is used to search specific cases for information about court appearances and case results. It includes only public information that would normally be provided by the court registry, such as accused name, file number, charges, and court appearances.	The public through JUSTIN Public Inquiry Terminals (JPTs) and other permitted bodies.
Trial Scheduling System (TSS) Module	The TSS module is used for maintaining judicial administrative information including the courtroom calendar for the Provincial Court and for checking the availability of police officers and Crown witnesses. It is linked to the Crown and Courts Modules.	Judicial case managers
Booking Maintenance Module (video conferencing)	The Booking Maintenance Module is used to book equipment for repair or other reasons.	Courts Services Branch staff
Booking Notification Module (video conferencing)	The Booking Notification Module is used to book video-conferences, equipment, and rooms.	Judicial case managers and Court Services Branch staff.
Law Enforcement Availability (LEA) Module	The LEA Module is used to enter personnel availability for trial scheduling purposes. It is linked to the TSS Module, Crown Module and RCC Module.	Criminal justice agencies, law enforcement agencies and the Judiciary
Reports Module	The Reports Module is used to produce reports such as the Accused History Report and Court lists.	Authorized JUSTIN users depending on their role
Justice Administration System (JAS) Module	Maintenance of JUSTIN tables.	JUSTIN Data Quality Unit, Systems Services Unit (JUSTIN support group) and Information Technology Services Division.

Figure 2 – The JUSTIN Application



## **PART B: Frequently Asked Questions**

### **1. What is electronic access to information in JUSTIN?**

---

Electronic access to JUSTIN is access to information in JUSTIN through a computer-to-computer link. A request for electronic access to JUSTIN is not the same as a request for information that may be contained in JUSTIN (see question 3 for information about non-electronic access to information in JUSTIN). Electronic access to JUSTIN is generally established for organizations that have an ongoing requirement to access information in JUSTIN or input information into JUSTIN.

### **2. Who may be permitted electronic access to JUSTIN?**

---

In order to ensure accountability, individuals will not be permitted electronic access to JUSTIN. Only organizations or agencies may be permitted electronic access to JUSTIN. An organization that receives electronic access may then designate specific personnel for access to JUSTIN.

### **3. What is non-electronic access to information in JUSTIN?**

---

Obtaining access to information in JUSTIN does not require a computer-to-computer link. Instead, the requested information may be provided in paper form or on a diskette. Those who do not have an ongoing requirement for access to information in JUSTIN may be provided information in this manner. For, example, information requested for research purposes may be provided this way.

#### 4. How do I apply for either electronic or non-electronic access to information in JUSTIN?

---

Regardless of whether you are requesting electronic or non-electronic access to information in JUSTIN, you should contact the Chair of the JUSTIN Access and Security Committee (JACS Committee) via email at: [AGCSBJACSCommittee@gov.bc.ca](mailto:AGCSBJACSCommittee@gov.bc.ca)

If you are requesting electronic access, then you should complete and submit the application form included in Part F of this package. Your application will be forwarded to the JACS Committee for review. A member of the JACS Committee may contact you for further clarification. The application form applies only to requests for electronic access to information in JUSTIN.

If you require non-electronic access to information in JUSTIN, you should send a letter as an email attachment to the Chair of the JACS Committee outlining the information required and the purpose of the request in as much detail as possible.

#### 5. Is there any way to access just the court record information contained in JUSTIN?

---

Yes. You do not need to apply for electronic or non-electronic access in order to access public court record information in JUSTIN. Instead, you may simply:

- (a) go to your local court house in person and request court record information in JUSTIN from court registry staff, or
- (b) in those courthouses that have a JUSTIN Public Inquiry Terminal (JPT) you may access public court record information directly from the JPT, or
- (c) view court lists on the Internet at <http://www.ag.gov.bc.ca/courts/court-lists/>

Please note that requests to court registry staff are generally restricted to a small number of cases in which an individual or an organization has a specific interest. Requests for non-electronic access to large quantities of public court record information should be addressed to the Chair of the JACS Committee (See Question 4 above).

---

## 6. What is a JUSTIN Public Terminal (JPT)?

---

A JPT is a computer terminal located in a courthouse, which provides the user with read-only access to court record information normally provided by the court registry. Information cannot be printed or downloaded. The primary purpose of providing access through a JPT is to provide short-term access to public information to individuals involved in a court proceeding.

---

## 7. What information can I access from a JPT?

---

Information available through a JUSTIN Public Inquiry Terminal (JPT) is court record information under the control of the Judiciary. JPTs in all court locations contain information about Supreme and Provincial Court adult criminal cases and other offences pursuant to provincial legislation.

The information that may be viewed through a JPT includes:

- participant names and aliases
- court file number
- agency file number (e.g. police file number)
- charges (counts, statute, description of offence)
- court appearance on each count (court location, level, date, time, room), reason for appearance and result of appearance including Judicial Interim Releases or detention
- final disposition.

## **8. What information is not accessible through a JPT?**

---

The following files or information are excluded from a JPT:

- information on youth cases
- all Applications
- witness names
- information on cases for which a pardon has been granted.

JPT searches will not provide any information on Supreme Court cases until an indictment has been filed.

A search for information on a case for which a pardon has been granted will return no information.

For searches on other excluded information or files, a message will be displayed on the screen informing the user that the file has a Limited Access restriction and to contact the registry for further information.

When a search is made on a case subject to a ban, the name of the accused will not be accessible.

## **9. Who decides who gets electronic access to JUSTIN and the scope of that access?**

---

The JUSTIN Access and Security Committee (JACS Committee) is responsible for determining who will be permitted electronic access to JUSTIN and the extent of that access. The JACS Committee is comprised of representatives from the Municipal police, provincial Crown counsel, courts, corrections, Judiciary, RCMP, and federal Crown counsel.

## **10. Who decides who gets non-electronic access to information in JUSTIN and what information they may access?**

---

The JUSTIN Access and Security Committee will forward requests for non-electronic access to information in JUSTIN to the appropriate body with authority over that information.

## **11. What factors are considered when deciding who will be granted electronic access to JUSTIN?**

---

When considering an application for electronic access to JUSTIN, the JUSTIN Access and Security Committee (JACS Committee) will review the specific information being requested and determine which module(s) of JUSTIN the applicant would need to access. The JACS Committee then applies the JUSTIN Electronic Access Policy, including the Criteria for Electronic Access to JUSTIN policy. See Part D of this package for an overview of the applicable policy on allowing electronic access to JUSTIN.

## **12. Will I have to sign an agreement for electronic access to JUSTIN?**

---

Yes. If an application for electronic access to JUSTIN is approved, a representative of the body receiving access will be required to sign an electronic access agreement before the access is implemented. This agreement will contain the terms and conditions of the electronic access to JUSTIN.

## **13. Will I have to sign an agreement for non-electronic access to information in JUSTIN?**

---

Yes. If your application for non-electronic access to information in JUSTIN is approved, you will be required to sign an agreement before the information is provided.

## **14. Will I have to pay for electronic access to JUSTIN?**

---

The body applying for access is expected to bear some or all of the costs to establish and maintain the electronic access, as determined by the JUSTIN Access and Security Committee in consultation with the body.

## **15. What are the technical requirements for electronic access?**

---

The technical requirements for electronic access to JUSTIN are outlined in Part C of this package.

## **16. How long will it take to process my application?**

---

The implementation schedule for JUSTIN is intensive, with priority for electronic access given to users such as police, Crown Counsel, courts staff, and corrections personnel. Consequently, even if your organization is approved for access, there may be a delay in your connection to JUSTIN. Applicants will be given an estimated timeframe for access when their access request is approved.

## **17. Who do I contact if I need more information?**

---

For more information about applying for access to JUSTIN, please contact the Chair of the JUSTIN Access and Security Committee via:

- Email: [AGCSBJACSCCommittee@gov.bc.ca](mailto:AGCSBJACSCCommittee@gov.bc.ca)
- Phone: (250) 356-1548
- Fax: (250) 356-8152

## PART C: Technical Requirements

### General

---

To access the JUSTIN application, the following is needed:

1. Microsoft Windows-based personal computer (PC)
2. A recent version of Microsoft Internet Explorer (IE) with Secure Socket Layer (SSL)
3. Oracle JInitiator plug-in is required. This is Oracle's version of Sun's Java Plug-In, which provides the ability to specify the use of a specific Java Virtual Machine on the client instead of using the browser's default JVM. Oracle JInitiator runs as an Active-X component in Internet Explorer.

### Network Connection

---

JUSTIN is accessed via an Internet connection. For security reasons, you must connect to the Provincial Government's Provincial Network (called SPAN/BC). For more information see the SPAN/BC website at [www.net.gov.bc.ca](http://www.net.gov.bc.ca).

### Installation

---

The Ministry of Attorney General will provide an installation guide. The organization receiving access will be responsible for installing the required software. The Ministry may assist by identifying technicians that are qualified to perform the installation. The organization receiving access will be responsible for all costs associated with installing the software.

## PART D: Policy on Allowing Electronic Access to JUSTIN

### Introduction

This part outlines the policy governing decisions on who will be provided electronic access to JUSTIN. It is taken from section 2.0 Criteria for Electronic Access to JUSTIN of the JUSTIN Electronic Access Policy.

This outline is intended to provide applicants with more information about how their application will be evaluated.

### Definitions

The definitions included here are used in the policy statements that follow and are critical for understanding the policy.

administration of the criminal justice system means:

- documenting, tracking, managing and processing of cases including prosecuting a case
- providing access to information consistent with legislation and Judicial policy and practice directives
- providing victims with information regarding the progress of cases relating to them, and
- creating statistics for management information and evaluation purposes.

authorized user means any individual who has signed an account access form, and:

- who is authorized to have electronic access to JUSTIN by an electronic access agreement or by an interim electronic access agreement
- who has electronic access to information in JUSTIN that is under their own authority, or
- whose electronic access to JUSTIN is otherwise approved by the JUSTIN Access and Security Committee (JACS Committee).

criminal case management means the tracking and processing of cases that would normally proceed through the criminal justice system including offences pursuant to provincial legislation.

criminal justice agency means municipal police, RCMP, Criminal Justice

Branch (MAG), Court Services Branch (MAG), Corrections Branch (MPSSG)<sup>1</sup>, Youth Justice (MCFD), the Federal Prosecution Service, B.C. Region, Department of Justice Canada (FPS) and includes bodies that have statutory authority to perform duties carried out by these bodies, or other bodies with a similar purpose as determined by the JUSTIN Access and Security Committee.

electronic court record means any information that is accessible through the Courts Module, Courts Inquiry Module, or Public Inquiry Module of JUSTIN.

Judiciary means the judges and staff that work for the B.C. Provincial Court and the Justices and staff that work for the B.C. Supreme Court and Court of Appeal.

law enforcement agency means a body that has a law enforcement mandate.

law enforcement mandate means that the body:

- has a specific statutory authority to conduct criminal and quasi-criminal investigations and recommend charges,
- has a specific statutory authority to supervise offenders in custody or in the community pursuant to sentences imposed by courts, or
- has employees with officer status under the provincial *Police Act* or similar federal legislation; this includes special provincial constables which have the same duties and powers as regular provincial constables under s. 9(3) of the *Police Act*.

law enforcement purpose means activities necessary to carry out the law enforcement mandate of a body.

public safety purpose within the context of electronic access means

- supervision and management of offenders or accused persons, and
- victim notification.

## Fundamental Purposes of JUSTIN

- (a) JUSTIN is an operational integrated criminal case management system and the electronic court record, to be used by criminal justice agencies and the Judiciary for public safety purposes, law enforcement purposes or the effective and efficient administration of the criminal justice system.
- (b) JUSTIN is used for Provincial Court criminal and civil trial scheduling.

---

<sup>1</sup> provincial Corrections Branch is included because they monitor for breaches of court orders and submit Reports to Crown Counsel for breaches of orders

## **General Limitations on Access**

When considering an application for electronic access to JUSTIN, the JUSTIN Access and Security Committee (JACS Committee) will review the specific information being requested and determine which module of JUSTIN the applicant would need to access. Then, the Committee will consider the following general limitations on access to specific JUSTIN modules.

### **Report to Crown Counsel (RCC) Module**

- a. Generally, unless the JACS Committee determines otherwise, electronic access to the RCC module will be limited to:
  - i. criminal justice agencies that create Reports to Crown Counsel
  - ii. law enforcement agencies that create Reports to Crown Counsel.

### **Crown Module**

- a. Generally, unless the JACS Committee determines otherwise, electronic access to the Crown module will be limited to:
  - i. Criminal Justice Branch, Ministry of Attorney General
  - ii. Federal Prosecution Service, B.C. Region, Department of Justice Canada, and
  - iii. Crown Agents contracted by the Federal Prosecution Service, B.C. Region, Department of Justice Canada, to perform prosecution services.

### **Courts Module**

- a. Generally, unless the JACS Committee determines otherwise, electronic access to the Courts module will be limited to:
  - i. specified CSB staff, and
  - ii. specified judicial administrative staff.

### **Courts Inquiry Module**

- a. Generally, unless the JACS Committee determines otherwise, electronic access to the Courts Inquiry Module will be limited to:
  - i. criminal justice agencies
  - ii. law enforcement agencies
  - iii. specified CSB staff, and
  - iv. specified judicial administrative staff.

### **Public Inquiry Module**

- a. Generally, unless the JACS Committee determines otherwise, electronic access to the Public Inquiry Module will be limited to:
  - i. electronic access through JUSTIN Public Terminals.

### **Trial Scheduling System (TSS) Module**

- a. Electronic access to the TSS module will be limited to:
  - i. the Provincial Court Judiciary, and
  - ii. Court Services Branch staff acting under the direction of the Provincial Court Judiciary.

### **Law Enforcement Availability (LEA) Module**

- a. Generally, unless the JACS Committee determines otherwise, electronic access to the LEA module, for the purpose of entering personal availability information, will be limited to:
  - i. law enforcement agencies, and
  - ii. criminal justice agencies.

### **Reports Module**

- a. Generally, unless the JACS determines otherwise, electronic access to the Reports module will be limited to bodies given electronic access to one or more other modules in JUSTIN.
- b. Electronic access to the Reports module will be determined by the role of the authorized user.

### **Booking Notification Module (video conferencing)**

- a. Electronic access to the Booking Notification Module will be limited to:
  - i. specified CSB staff, and
  - ii. Judicial case managers (trial schedulers).

### **Booking Maintenance Module (video conferencing)**

- a. Electronic access to the Booking Maintenance Module will be limited to specified CSB staff.

### **Justice Administration System (JAS) Module**

- a. Electronic access to the JAS Module will be limited to the:
  - i. JUSTIN Data Quality Unit
  - ii. Systems Services Unit (JUSTIN Support Group)
  - iii. Information Technology Services Division.

## Criteria for Electronic Access to JUSTIN

In addition to the general limitations noted above, the JACS Committee will consider the following criteria when reviewing an application for electronic access.

- a. Electronic access to JUSTIN may be permitted to bodies that:
  - i. fall within the fundamental purposes of JUSTIN
  - ii. have a law enforcement mandate and request access to JUSTIN for law enforcement or public safety purposes
  - iii. request electronic access for the purpose of complying with the *Victims of Crime Act*
  - iv. request electronic access to case status information in order to provide this information to victims where the request is consistent with legislation and Judicial policy and practice directives regarding electronic access to court record information
  - v. request electronic access to information that is in the public domain where the request is consistent with legislation and Judicial policy and practice directives regarding electronic access to court record information, or
  - vi. require access to the Law Enforcement Availability (LEA) Module in order for the Provincial Judiciary to schedule trials.
- b. If electronic access may be permitted under the criteria above, the JACS Committee will consider:
  - i. whether the request for access is consistent with law
  - ii. whether the request is consistent with applicable policy
  - iii. whether the body has demonstrated that the requested access is for a legitimate work-related purpose
  - iv. whether permitting the access will enhance the efficiency and effectiveness of the criminal justice system
  - v. whether, where applicable, the body will agree to enter required information into JUSTIN
  - vi. whether the benefit of the electronic access is sufficient to justify any costs, not borne by the applying body, associated with establishing the access
  - vii. the means by which the body is currently accessing or submitting the information or will need to access or submit the information in the immediate future
  - viii. the frequency with which the body is currently accessing or submitting the information or will need to access or submit the information in the immediate future, and
  - ix. the volume of information that the body is currently accessing or submitting or will need to access or submit in the immediate future.

before deciding whether to permit electronic access to JUSTIN.

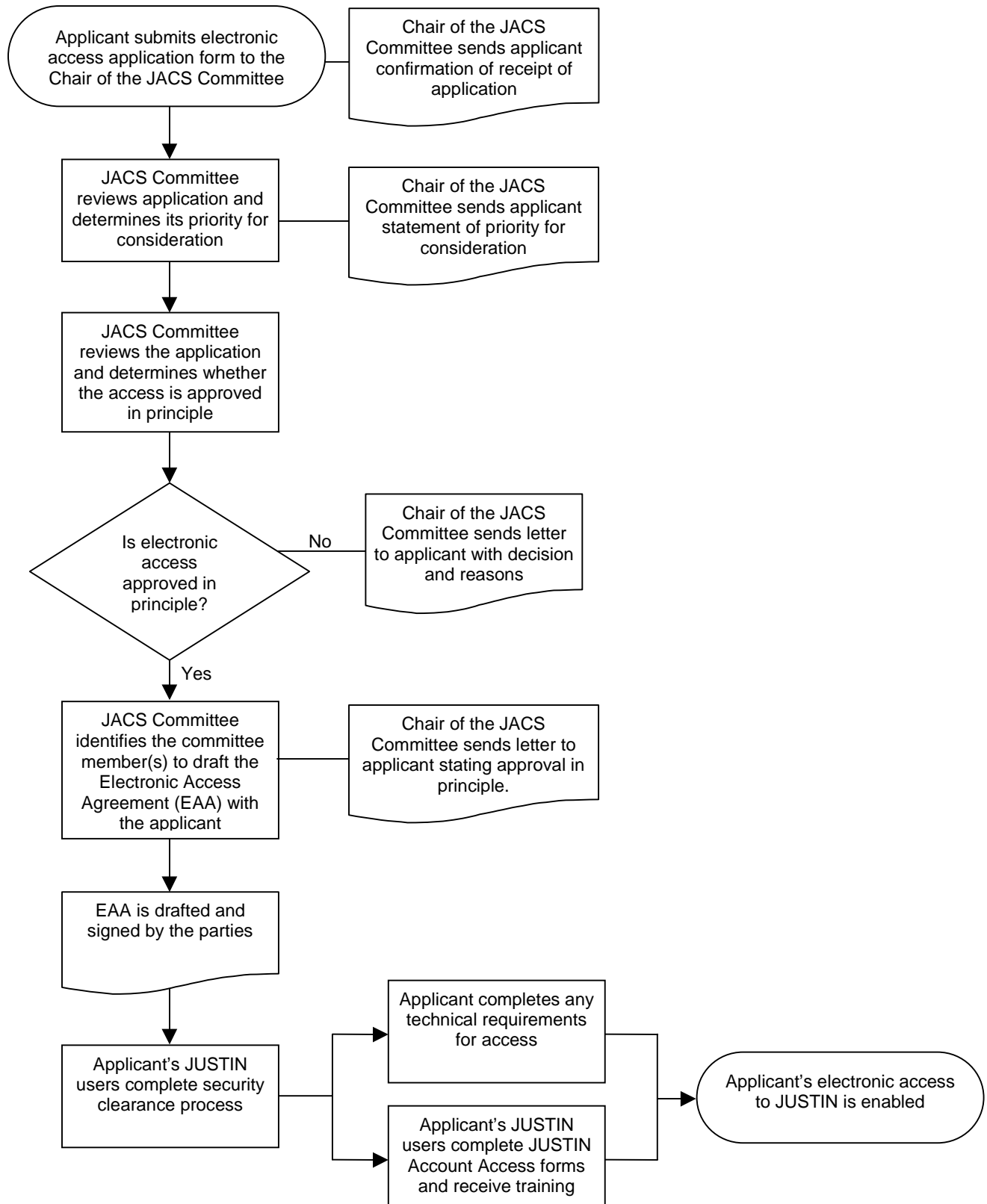
## **Technical Functionality of JUSTIN**

Regardless of whether an applicant meets the criteria noted above, electronic access to JUSTIN will be denied to an otherwise eligible body if the technical functionality of JUSTIN cannot support the parameters of the requested access. For example, if, where applicable, a body's access cannot be limited only to those cases in which the body has a legitimate work-related purpose, electronic access will be denied.

## **Costs**

The body applying for electronic access is expected to bear some or all of the costs to establish and maintain the electronic access, as determined by the JACS Committee in consultation with the body. These might include training, network costs, upgrades to software or hardware, or other systems changes.

## PART E: Application Process Flowchart



## PART F:

### APPLICATION FORM FOR ELECTRONIC ACCESS TO JUSTIN

Please complete this application form electronically and send as an email attachment to the Chair of the JUSTIN Access and Security Committee at: [AGCSBJACSCCommittee@gov.bc.ca](mailto:AGCSBJACSCCommittee@gov.bc.ca)

In order for your request to be considered, you must answer all questions in full.

**Name of Organization:**

**Address:**

**Contact Name:**

**Contact Position:**

**Telephone:**

**Fax:**

**E-mail:**

1. What is the mandate of your organization?
2. What is your organization's statutory or policy authority for operations, if any?
3. Please describe the general nature of your organizations work and the specific nature of operations requiring access to information in JUSTIN, including the number and location of offices (Note: Applications for electronic access to JUSTIN must be made by an organization's head office).
4. Is the computer system through which your organization would access JUSTIN currently interfaced with any other computer systems?  
 Yes  
 No

If yes, please describe.

5. Has your organization ever had electronic access to JUSTIN that has been revoked?

- Yes
- No

If yes, please provide details.

6. Please indicate which of the following types of electronic access to JUSTIN your organization is requesting?

- Ability to view information only, e.g. court results. No ability to input information or modify information (read-only electronic access).

Please list the information your organization wishes to access. Be as specific and detailed as possible.

- Ability to create (input) information into JUSTIN, e.g. Law Enforcement Availability (shared-management access).

Please list the information your organization wishes to input into JUSTIN. Be as specific and detailed as possible.

- Ability to modify information in JUSTIN, e.g. changing, or deleting information (shared-management access).

Please list the information your organization wishes to modify in JUSTIN. Be as specific and detailed as possible.

7. How would the information you wish to access from JUSTIN be used by your organization in light of its mandate and the specific nature of its operations as described in Question 1 and 3 above? Please be as specific as possible.

8. Do any of your employees who would access JUSTIN have officer status under the provisions of the provincial *Police Act* or federal legislation?

- Yes
- No

If yes, please provide the Act and section number of the provisions granting access:

**9. Do any of your employees prepare Reports to Crown Counsel (RCCs)?**

- Yes
- No

If yes, please provide the approximate number of RCCs prepared per year:

**10. Is your organization authorized to view youth records in accordance with the *Youth Criminal Justice Act* or regulations pursuant to the Act?**

- Yes
- No

If yes, please provide the section number and/or OIC number of the provision granting authority:

**11. Does your organization have any specific statutory authority to access and/or use the information you wish to access from JUSTIN?**

- Yes
- No

If yes, please provide the Act and section number of the provision granting authority:

**12. Does your organization currently obtain the information that you wish to access in JUSTIN from another source?**

- Yes
- No

If yes, please describe how you currently obtain this information:

**13. Approximately how many people in your organization would require access to JUSTIN?**

Please provide a breakdown of this number by occupational position and office location, and indicate approximately how often each would need to access information in JUSTIN (e.g. daily, weekly, monthly, or less than monthly).

Position	Office Location	Number	Frequency

**14. Does your organization require its employees/contracted workers to have a security clearance?**

- Yes
- No

**If yes, please describe (i) the type of clearance (e.g. name check, fingerprint, background check), (ii) who conducts the clearances (e.g. RCMP, Municipal police) and (iii) how frequently the security clearances are conducted.**

**15. Please describe the physical security of your office building and office space (e.g., security guards, electronic pass cards).**

**16. Is your organization bound by any privacy legislation?**

- Yes
- No

**If yes, what Act?**

**If no, what policies are in place to ensure the protection of personal information?**

**Note: you may be required to complete a Privacy Impact Assessment (PIA) as part of your application for electronic access to JUSTIN.**

**Name:**

**Title:**

**Date:**

**Please send your completed application form via email attachment to the Chair of the JUSTIN Access and Security Committee at:**

[AGCSBJACSCCommittee@gov.bc.ca](mailto:AGCSBJACSCCommittee@gov.bc.ca)

## 2.0 JACS Committee Evaluation Guide for Applications for Electronic Access

To obtain a copy of this Evaluation Guide, please send an email request to:  
[AGCSBJACSCommittee@gov.bc.ca](mailto:AGCSBJACSCommittee@gov.bc.ca)



**ELECTRONIC ACCESS TO  
INFORMATION IN JUSTIN**

**Evaluation Guide for Electronic Access  
Applications to JUSTIN**

**JUSTIN Access and Security Committee**

## IMPORTANT – PLEASE READ BEFORE USING THIS GUIDE

The purpose of this document is to assist the JUSTIN Access and Security Committee (JACS Committee) in evaluating applications for electronic access to JUSTIN.

Evaluating applications for electronic access may require discussion with applicants, the Judiciary, ITSD or legal counsel. Often, it will not be a linear process. Consequently, while this document sets out 7 steps for the JACS Committee to complete when evaluating applications, these steps will not always take place sequentially. The evaluation criteria in the JUSTIN Electronic Access Policy should be considered as a whole when analyzing an application for electronic access.

Name of body applying for electronic access: \_\_\_\_\_

Contact person: \_\_\_\_\_

Title: \_\_\_\_\_

Telephone: \_\_\_\_\_

E-Mail: \_\_\_\_\_

Date application was received: \_\_\_\_\_

Comments:

---

---

---

## STEP 1

---

Determine what information the applicant is requesting and the module of JUSTIN from which the information would be accessed.

Information Requested <i>e.g. name, charge type</i>	Module	Comments

## STEP 2

---

Review the application form and the **General Limitations on Electronic Access** in sections 2.2.7 to 2.2.16 of the policy 2.0 **Criteria for Electronic Access to JUSTIN** to determine if the applicant qualifies for access to the module(s) identified in Step 1.

Comments:

- *If the applicant is requesting electronic access to a module with limited access – and they are not a permitted body – **STOP**. Send the applicant a letter declining the request for electronic access to JUSTIN.*
- *If the applicant is requesting electronic access to a module that has general limitations on access – and the applicant is not the type of body that generally is permitted access to the module(s) in question, this should be considered as part of the decision-making process. The JACS Committee may still determine that the body may have access despite the general limitation on access stated in the policy. **PROCEED TO STEP 3**.*

### STEP 3

---

Does the applicant meet at least one of the criteria for permitting access in section 2.2.3(a) of the policy 2.0 Criteria for Electronic Access to JUSTIN?

Comments:

- *If none of the six criteria above are met – **STOP**. Send the applicant a letter declining the request for electronic access to JUSTIN.*
- *If at least one of the criteria is met, **PROCEED TO STEP 4**.*

### STEP 4

---

Does the access meet all of the criteria in the subsections of section 2.2.3(b) of the policy 2.0 Criteria for Electronic Access to JUSTIN?

Comments:

- *If all of the criteria above are not met, the JACS Committee will decide whether or not to continue evaluating the application. If the JACS Committee decides not to continue evaluating the application – **STOP**. Send the applicant a letter declining the request for electronic access to JUSTIN. If the JACS Committee decides to continue evaluating the application, **PROCEED TO STEP 5**.*
- *If all of the criteria in STEP 4 are met, **PROCEED TO STEP 5**.*

## STEP 5

---

Does the technical functionality of JUSTIN support the access as required in section 2.2.4 of the policy 2.0 Criteria for Electronic Access to JUSTIN?

Comments:

- *If the requested access cannot be supported by the technical functionality of JUSTIN – **STOP**. Send the applicant a letter declining the request for electronic access to JUSTIN.*
- *If the requested access can be supported by the technical functionality of JUSTIN, **PROCEED TO STEP 6**.*

## STEP 6

---

Does the requested access present an unacceptable risk to the information in JUSTIN as determined under the policy 6.0 Security for Electronic Access to JUSTIN?

a. **Should a security threat and risk assessment be conducted on the requested access?**  
(See Part B, s. 6.2.5(a)).

- *If 'Yes', then the JACS Committee should request that ITSD conduct a security threat and risk assessment.*
- *If 'No', **PROCEED TO STEP 7**.*

b. **Has the security threat and risk assessment exposed an unacceptable risk to the information in JUSTIN?**

- *If the JACS Committee determines that the security threat and risk assessment has exposed an unacceptable risk to the information in JUSTIN, the electronic access will not be permitted – **STOP**. Send the applicant a letter declining the request for electronic access to JUSTIN.*
- *If the JACS Committee determines that the security threat and risk assessment has not exposed an unacceptable risk, **PROCEED TO STEP 7**.*

## **STEP 7**

---

- *The application has been approved in principle.*
- *The JACS Committee should determine which committee member(s) will be responsible for drafting the EAA with the applicant, and the extent of the security clearances that will be required for the applicant's JUSTIN users.*
- *Send the applicant a letter (see Letter #4 in 3.0 Form Letters,) informing them that the application for electronic access to JUSTIN has been approved in principle.*

## 3.0 Form Letters

**Letter #1**  
**To Applicant acknowledging receipt of the electronic access application**

[CSB letterhead]

[CSB file number]

[Date]

[Name of applicant  
address of applicant]

Dear [applicant]:

Re: Request for Electronic Access to JUSTIN by [body name]

Thank you for your request for electronic access to JUSTIN dated [X] and received in my office on [date].

The JUSTIN Access and Security Committee will be meeting within a month to review new applications for JUSTIN and will conduct a preliminary review and determine the priority of your request at that time. A follow-up letter will be sent to you after the JUSTIN Access and Security Committee has met.

Sincerely,

Virginia Day  
Chair  
JUSTIN Access and Security Committee

**Letter #2**

**To Applicant re priority for consideration of the application for electronic access**

[CSB letterhead]

[CSB file number]

[Date]

[Name of applicant  
address of applicant]

Dear [applicant]:

Re: Priority for considering [body's name] request for Electronic Access to JUSTIN

Thank you for your request for electronic access to JUSTIN dated [X] and received in my office on [date].

The JUSTIN Access and Security (JACS) Committee met on [X] to review applications for electronic access to JUSTIN and to determine their priority for consideration.

The JACS Committee will be considering your application for electronic access to JUSTIN [immediately/next month/date] and will be in contact with you once the review is completed.

Sincerely,

Virginia Day  
Chair  
JUSTIN Electronic Access Committee

**Letter #3**  
**To Applicant declining application for electronic access to JUSTIN**

[CSB letterhead]

[CSB file number]

[Date]

[Name of applicant  
address of applicant]

Dear [applicant]:

Re: Request for Electronic Access to JUSTIN by [body name]

Thank you for your request for electronic access to JUSTIN dated [X] and received in my office on [date].

The JUSTIN Access and Security Committee (JACS Committee) met on [X] to review the [body's name] application for electronic access to JUSTIN. During that review, the JACS Committee determined that [body name] does not meet the criteria for electronic access to JUSTIN because [details].

Sincerely,

Virginia Day  
Chair  
JUSTIN Access and Security Committee

**Letter #4**

**To Applicant confirming approval in principle of application for electronic access**

[CSB letterhead]

[CSB file number]

[Date]

[Name of applicant  
address of applicant]

Dear [applicant]:

Re: Request for Electronic Access to JUSTIN by [body name]

Thank you for your request for electronic access to JUSTIN dated [X] and received in my office on [date].

The JUSTIN Access and Security (JACS) Committee met on [X] to review the [body's name] application for electronic access to JUSTIN. During the review, the JACS Committee determined that [body name] meets the criteria for electronic access to JUSTIN and the application for electronic access was approved in principle.

[JACS Committee member name(s), branch/organization] will be contacting you shortly to discuss drafting an electronic access agreement for electronic access to JUSTIN. I have attached a copy of the Electronic Access Agreement (EAA) template for your review.

Sincerely,

Virginia Day  
Chair  
JUSTIN Access and Security Committee

## 4.0 Memos

## MEMORANDUM

September 9, 2003

**TO:** All JACS Committee Members

**FROM:** JUSTIN Access and Security Committee

**RE:** **Disabling or deleting a JUSTIN Account**

Outlined below is the process for permanently deleting or temporarily disabling a JUSTIN account. Each JACS Committee member is responsible for ensuring that their body/agency has this information and implements this process:

- if an employee no longer requires electronic access to JUSTIN - either temporarily or permanently - it is the task of the body responsible for the user to send a request to ITSD to have the account access disabled.
- if a user will not be accessing their JUSTIN account for up to 3 months because they are, for example, on leave, it is not necessary to contact ITSD to have the account temporarily disabled.
- if a user will not be accessing their JUSTIN account for a period longer than 3 months please contact ITSD using the process outlined below and request that the access be temporarily disabled.

To permanently delete or temporarily disable a JUSTIN account you must:

1. tick (✓) either 'delete' or 'disable' at the top of page 1 of the Account Access Form (see attached) and provide a brief explanation as to why the account should be deleted or temporarily disabled, e.g. 'retired', 'no longer employed', 'on leave'.
  2. fill out the relevant sections of the MAG, ITS Account Access Form - only page 1 needs to be completed
  3. have a person in authority sign the form to approve the request for deletion/disabling
  4. fax page 1 to (250)-356-5210 attention to Tanya Patterson.
- When an employee is returning to service or will again require access to JUSTIN, it is the task of the body responsible for the user to request that the JUSTIN access be enabled again.

## 5.0 JUSTIN Public Inquiry Terminal Use Notice



## NOTICE PUBLIC TERMINAL USE

### Prohibited use

Public use of this computer system is provided for access to case activity information and courtroom location only. Any other use of this computer system is expressly prohibited. Persons found misusing this privilege will lose access to the system and may be subject to legal action, including prosecution.

### Disclaimer

Every effort is made to ensure that the information posted on this system is or remains consistent with statutory and court-ordered publication and disclosure bans. However, the posting of this information is in no way a representation, express or implied, that the information conforms to publication and disclosure bans. As bans may be granted at any stage in the proceeding, the posted information will not include details of a ban granted in court on that day. Therefore, to ensure compliance with court-ordered bans, it is the responsibility of the users of this public terminal and of those relying on the information posted to personally check with the applicable court clerk or court registry for court-ordered bans on publication or disclosure.

Publication or disclosure of information contrary to a court-ordered ban may result in legal action, including prosecution.

## 6.0 Account Access Form

To obtain a copy of this Account Access Form, please send an email request to: [AGCSBJACSCCommittee@gov.bc.ca](mailto:AGCSBJACSCCommittee@gov.bc.ca)



MINISTRY OF ATTORNEY GENERAL  
INFORMATION TECHNOLOGY SERVICES (ITS)  
**ACCOUNT ACCESS FORM**

FAX BOTH SIGNED PAGES TO (250) 356-5210

Create       Delete       Modify       Transfer

**USER DETAILS**

<u>Last Name</u>	<u>Employee #</u>	Regular <input type="checkbox"/> Auxiliary <input type="checkbox"/>
<u>First Name</u> <u>Initial</u>	<u>Title</u>	Contractor <input type="checkbox"/> Co-op <input type="checkbox"/>
<u>Branch</u>	<u>Phone #</u>	<u>Start Date</u> mm/dd/yyyy
<u>Division</u>	<u>FAX #</u>	<u>End Date</u> mm/dd/yyyy
<u>Address</u>	<u>City</u>	<u>Postal Code</u>
<u>Transfer from Address</u>		

**ATTORNEY GENERAL ACCESS**

<input type="checkbox"/> E-Mail (specify)	<u>Applications (list)</u>	<u>Training Complete?</u>
		Yes <input type="checkbox"/> No <input type="checkbox"/>
<input type="checkbox"/> IDIR (Same as eg. Jane Doe)		Yes <input type="checkbox"/> No <input type="checkbox"/>
		Yes <input type="checkbox"/> No <input type="checkbox"/>
Internet Proxy YES <input type="checkbox"/> NO <input type="checkbox"/>	IPP ID YES <input type="checkbox"/> NO <input type="checkbox"/>	IPP Group Name _____

**CORP ITSD ACCESS**

<input type="checkbox"/> MVS Systems (BC ONLINE/RMS etc)	<u>Client #</u>	<u>Charge #</u>
<input type="checkbox"/> Spandial		
<u>Specific Information for Access</u>		

**AUTHORIZATION**

<u>Authorizing Signature</u>	<u>Name</u>	<u>Date</u>
Not Applicant's Signature	Please Print	

The authorizer is informed via e-mail once account is created.  
Dormant accounts of one year or more will be removed from the system.

**ITSD USE ONLY**

<u>UserID</u>	<u>Created</u>
<u>IDIR</u>	<u>OAMS</u>
<u>E-Mail</u>	<u>ORACLE</u>
<u>UNIX</u>	<u>Comments</u>
<u>Proxy / Other</u>	
	Notified? Yes <input type="checkbox"/> No <input type="checkbox"/>

**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* (see General Management Operating Policy Chapter 3.5.13 and BC Archives and Record Services, Records Information Management manual Policy No. 5.13/01).

**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
_____	_____	_____
Applicant's Signature	Please Print	