JUSTIN ACCESS AND SECURITY COMMITTEE

Do you use JUSTIN at work?

If you answered 'yes' then read this brochure for important information regarding the JUSTIN Electronic Access Policy and its impact on JUSTIN users on a day-to-day basis.

This brochure is distributed for the use of people that use JUSTIN at work.

Table of Contents

Who should read this brochure?

You should read this brochure if you use JUSTIN as a part of your work. Some examples of JUSTIN users are:

- B.C. Ministry of Attorney General, Court Services Branch staff
- B.C. Ministry of Attorney General, Criminal Justice Branch staff
- B.C. Ministry of Public Safety and Solicitor General, Corrections Branch staff
- B.C. Ministry for Children and Family Development, Youth Corrections staff
- B.C. Provincial Crown Counsel
- Federal Crown Counsel
- Federal Crown agents
- B.C. Municipal police
- RCMP
- B.C. police-based victim service workers
- Various law enforcement officers that enforce provincial and federal statutes

Why should you read this brochure?

The JUSTIN Electronic Access Policy has an impact on JUSTIN users. This brochure explains what you need to know about how the JUSTIN Electronic Access Policy affects you on a day-to-day basis.

Who wrote the JUSTIN Electronic Access Policy?

The JUSTIN Access and Security Committee (JACS Committee) wrote the JUSTIN Electronic Access Policy. The JACS Committee is the committee responsible for managing access to JUSTIN. This includes writing the policy that governs JUSTIN and making decisions on who gets access to JUSTIN.

The JUSTIN Access and Security Committee has representatives from the:

- B.C. Ministry of Attorney General, Criminal Justice Branch
- B.C. Ministry of Attorney General, Court Services Branch
- B.C. Ministry of Public Safety and Solicitor General, Corrections Branch
- B.C. Ministry of Attorney General and Ministry of Public Safety and Solicitor General, Information Technology Services Division
- B.C. Municipal Police
- RCMP
- B.C. Provincial Court Judiciary
- B.C. Supreme Court Judiciary
- Federal Prosecution Service, Department of Justice

All of these organizations participated in writing the JUSTIN Electronic Access policy.

What is the JUSTIN Electronic Access Policy?

The JUSTIN Electronic Access Policy guides decisions about permitting, managing and revoking electronic access to JUSTIN.

The JUSTIN Electronic Access Policy manual is published in its entirety on the Internet at:
http://www.ag.gov.bc.ca/courts/manuals/justin/

How does the JUSTIN Electronic Access Policy affect JUSTIN users on a day-to-day basis?

There are 4 key JUSTIN policies that affect JUSTIN users on a day-to-day basis:

1. Security for Electronic Access to JUSTIN
2. Audit Trails and Audits for Electronic Access to JUSTIN
3. Unauthorized Use of Electronic Access to JUSTIN, and
4. Revoking Electronic Access to JUSTIN.

This section of the Guide outlines the key features of these 4 JUSTIN Electronic Access policies but it **does not replicate them in their entirety** from the JUSTIN Electronic Access Policy and Procedures Manual.

#1 Security for Electronic Access to JUSTIN

The Security for Electronic Access to JUSTIN policy requires that JUSTIN users will:

undergo a security clearance as specified by the policy

A security clearance means, at a minimum, a criminal record name check. Depending upon the information that you have access to in JUSTIN, a security clearance may include a more comprehensive background check as well. Your consent is required for any type of security clearance and you will be advised of the type of security clearance that your work requires before one is conducted.

maintain workstation security as specified by the policy

This means that you will not leave your terminal unattended when you are logged-on to JUSTIN and you will terminate active sessions when you are finished unless they can be secured by a locking mechanism, e.g. password protected screen savers. It is the responsibility of your employer to tell you what you must do to maintain workstation security.

report any security incidents to the appropriate person at your place of work

It is the responsibility of your employer to establish and tell you the procedures for reporting any breaches of security in your workplace.

#2 Audit Trails and Audits

JUSTIN automatically creates audit trails of JUSTIN usage; this is to help protect the information in JUSTIN by ensuring that JUSTIN users are accountable for their use of electronic access. An audit trail is sometimes called an ‘electronic fingerprint’ because when you use JUSTIN, the system links your username with your activity. This means that whenever you create, modify

or delete information in JUSTIN this can be traced to you through your username.

Some, but not all, viewing of information in JUSTIN also creates an audit trail.

From time-to time, compliance audits will be conducted to help keep JUSTIN secure. A compliance audit means that a type of information (e.g. witness names), or a group of users (e.g. Crown Counsel), would be audited to ensure that all access and use of JUSTIN was authorized.

A compliance audit does not target individual users. However, if you were suspected of unauthorized use of electronic access to JUSTIN then a targeted audit may be conducted on your use of JUSTIN.

#3 Unauthorized Use of Electronic Access to JUSTIN

Unauthorized use of electronic access to JUSTIN is serious; JUSTIN contains sensitive criminal justice information. If unauthorized use of electronic access to JUSTIN occurs, it could result in harm, including compromising public safety and the administration of justice. The *Unauthorized Use of Electronic Access to JUSTIN* policy is strictly enforced.

The *Unauthorized Use of Electronic Access to JUSTIN* policy defines 'unauthorized use' and explains what will happen if a JUSTIN user is suspected of unauthorized use of JUSTIN.

The *Unauthorized Use of Electronic Access to JUSTIN* policy applies to intentional unauthorized use; it does not apply when you make a data entry error or access information inadvertently due to inexperience or human error.

What is an 'unauthorized use' of electronic access to JUSTIN?

An unauthorized use is defined in the policy as including:

creating, viewing, modifying, using, disclosing or deleting information beyond the scope of the permitted access, or for an unauthorized purpose

Example: you have the authority to modify an accused's name (e.g. to correct a spelling error) but you intentionally modify an accused's name so that a search against the real name comes up empty.

Example: you view some information that you have the authority to view but then you disclose what you have seen to someone in a social context, e.g. you tell an acquaintance about someone else's criminal record.

electronic access by an authorized user during the course of carrying out their duties that is not a legitimate work-related use consistent with the conditions of employment or terms of contract

Example: while at work, you go into JUSTIN to see whether a social acquaintance has a criminal record.

Example: while at work, you go into JUSTIN to see what new developments there may be in an interesting or high profile criminal case.

violating the terms of the Account Access Form including:

i. divulging, sharing or compromising a password

Example: telling someone your password.

Example: logging on to JUSTIN and then allowing another person to access JUSTIN under your username and password.

Example: writing your password somewhere where another person can access it easily.

ii. using another individual users' username

Example: you log onto JUSTIN using another person's username and password.

Example: one person logs on to JUSTIN then you access JUSTIN under that person's username.

What happens when an incident of suspected unauthorized use occurs?

All unauthorized use of JUSTIN is investigated. An investigation may be as simple as your supervisor noticing that you are sharing your username and reviewing the access policy with you: it may also be as complex as a full criminal investigation. The nature and extent of the investigation depends on the unauthorized use that is identified or suspected.

If you are suspected of unauthorized use of JUSTIN, your employer will decide whether to suspend your access to JUSTIN pending the investigation. The *Unauthorized Use of Electronic Access to JUSTIN* policy sets out the criteria that your employer will consider when making this decision.

If the investigation concludes that an unauthorized use did not occur, the matter is closed. If the investigation concludes that an unauthorized use did occur, then your employer will take appropriate action pursuant to the JUSTIN Electronic Access Policy and the policies and procedures of your employer.

Appropriate action may include suspending your electronic access for a specified period of time, changing your type of access, revoking your access or any action that is permissible under the terms and conditions of your employment.

#4 Revoking Electronic Access to JUSTIN

Your employer may revoke your electronic access to JUSTIN for unauthorized use of electronic access if that is the most appropriate action given the nature of your unauthorized use. Your employer may subsequently reinstate your electronic access to JUSTIN. The *Revoking Electronic Access to JUSTIN* policy sets out the criteria that your employer will consider when making these decisions.

Questions?

If you have any questions about the JUSTIN Electronic Access Policy, you should ask your employer for clarification. If your employer cannot answer your question, they should send the question to the Chair of the JUSTIN Access and Security Committee at:

AGCSBJACSCommittee@gems7.gov.bc.ca