WASHINGTON COURTS

October 26, 2018

TO: JISC Data Dissemination Committee

FROM: Stephanie Happold, AOC Data Dissemination Administrator

RE: Non-Court IT Personnel JIS Access Policy

Background

AOC staff originally brought this issue to the Committee in 2014. The agency was receiving increased requests from courts to give JIS access to non-court IT personnel, and asked the Committee for a policy on how to handle the access. During its June 24, 2014 meeting, the Committee decided that while it continued to discuss the matter, AOC was to provide temporary JIS RACFIDs that were limited to six months and did not extend to creating BOXI reports. The policy was then tabled. AOC staff is requesting a Committee review of the temporary policy in conjunction with JIS General Policy 4.1.9, as the temporary access is just being renewed every six months until a permanent solution is provided. Below are the Committee meeting minutes discussing the policy and applicable JIS General Polices. Questions to be discussed are:

-is the temporary exemption still needed?
-are there any other services the non-court IT personnel provide courts/county clerks that are not described in JIS General Policy 4.1.9?
-is the 4.1.9 process too time-consuming for some situations?
-do non-court IT personnel need access to eservice?

DDC Meeting Minutes

February 28, 2014, meeting minutes:

4. Access to JIS for Non-Court IT Employees Staff is seeking direction from the DDC in granting JIS access to local government non-court IT personnel. There is an increase of court requests for court RACFIDs to be issued to non-court IT employees for reasons ranging from detailed explanations of particular projects for court-related computer systems, to needing constant access for the IT personnel who assist with the local government network communicating with the court system, to simply stating that the IT personnel need access to assist in computer systems. AOC is finding it increasingly difficult to sort and review these requests and decide which ones are based on court-needs and which requests are for convenience sake only. Furthermore, AOC has

concerns about how the courts are setting up these profiles. The Committee requested that staff provide recommendations on possible criteria that may be used in granting these requests. The Committee will then review the criteria at the next meeting and provide guidelines based on staff's suggestions. Judge Heller will also review how Pierce County handles JIS access for non-court IT personnel and report back to the Committee.

April 25, 2014, meeting minutes:

4. Access to JIS for Non-Court IT Employees AOC has been contacted by several courts requesting access to JIS by their county/city IT departments. In most of these situations, the IT departments are non-court employees. They are usually employed by the municipality or the county. Aimee Vance gave an example of Kirkland Municipal Court's need to use City of Kirkland IT employees to assist the court in a move of computers. Ms. Vance stated she needed the expertise of the city IT employees to do the work. The Committee agreed that such work is a necessity, but stated the access should be limited and should be time blocked. They agreed with the recommendations that Ms. Happold set forth in her memo and suggested that she develop a form/application (consulting with AOC security) that the administrator/clerk complete prior to awarding access. Judge Leach also suggested drafting guidelines that explain when such requests would be granted and what criteria would be considered. They ask that Ms. Happold draft an application/form and bring it to the next meeting for their approval.

June 27, 2014, meeting minutes:

2. Access to JIS for Non-Court IT Employees The Data Dissemination Committee continued its discussion about JIS access for noncourt/clerk local government IT personnel. Proposed guidelines for providing access were reviewed. Barb Miner, Aimee Vance and DDA Stephanie Happold were tasked with creating a survey for clerks and court staff to provide the Committee information about what access is needed. While the Committee continues to discuss this matter, it authorized AOC to provide temporary RACFIDs to non-court/clerk local government IT personnel. The temporary access is limited to six months and does not extend to using IT personnel for creating BOXI reports. If BOXI reports are needed, the court/clerk can contact AOC for assistance.

September 5, 2014, meeting minutes:

2. Access to JIS for Non-Court IT Employees The Data Dissemination Committee continued its discussion about JIS access for noncourt/clerk local government IT personnel. Results from the survey sent to clerks and court staff were discussed. AOC staff will find out if providing DVOL access instead of PROD will protect JIS security. Also, Barb Miner will ask her IT personnel what sort of JIS access is needed and why. Last, the Committee asked AOC staff if training for court staff and clerks could be provided on JISC and DDC policies, RACFIDs, and JIS use.

October 24, 2014, meeting minutes:

6. RACFID Training The Committee discussed developing a training for Court Administrators and Clerks on RACFID set-up, use, maintenance, and data confidentiality. AOC staff is to continue working on the draft power point presentation for the next meeting and to schedule the presentation for the upcoming Court Administrators and Clerks' trainings

7. Access to JIS for Non-Court IT Employees The Data Dissemination Committee decided to table this topic for a later date.

March 6, 2015 meeting minutes:

2. Spokane Request for RACFIDs for IT Personnel Mr. Ronald Miles presented Judge Cozza's request to allow three non-court IT personnel permanently assigned to the Spokane Superior Court to be given RACFIDs for continued work with the County Courts and Clerk's Office. Barb Miner asked DDA Happold why her recommendation stated this request was different than the other requests that are under the temporary access provided to non-court/clerk IT personnel by the DDC during its June 27, 2014 meeting. DDA Happold responded that Spokane's IT personnel are permanently assigned to the courts for work related only to court/clerk activities. The personnel will not be partitioned between executive branch and judicial branch. Also, employees will not be rotated in and out of the projects; the access will only be for these three. The Committee voted unanimously to allow the three non-court IT personnel permanently assigned to the Spokane Superior Court to be given RACFIDs for work with the County Courts and Clerk's Office.

<u>JIS General Polices</u>

JIS General Policies (with Annotations)

4.1 Access Rules

4.1.1 Access to the JIS

Except for public access programs such as JIS-Link and the Washington Courts (www.courts.wa.gov) Internet website, access to the JIS computer systems is restricted to authorized personnel who have been assigned a JIS user account. For courts and county clerks, JIS Site Coordinators, under the direction of the county clerk or court administrator, are authorized to assign JIS accounts to individual court or county clerk employees. Such assignments shall be based on each employee's work responsibilities and business need for access and other privileges.

4.1.2 Update Privileges

Information in the JIS database may be updated by court and county clerks' office personnel only. All others shall be restricted to read-only access.

4.1.3 Court User IDs

Courts and county clerks may assign user IDs to their employees only. Only court employees may have court level access and update privileges associated with court user IDs.

4.1.4 User Account Deactivation

It is the responsibility of the site coordinator to deactivate an employee's user account (user id and password) upon termination of the employee's employment. Such deactivation must be done at the time the employee last leaves the court or clerk's office premises, regardless of when the employee actually leaves the payroll.

4.1.5 User Responsibilities

Users shall respect the privacy of other JIS network users and the integrity of their data. Users shall not seek information on other users; obtain copies of or modify files, other data, or passwords belonging to other users; or represent themselves as another user.

4.1.6 Password Locked Screensavers

Password locked screensavers shall be used on all personal computers connected to the JIS from the courts, or connected to the AOC network and must be set to initiate the screensaver no more than 15 minutes after the last use.

COMMENT

This control is necessary to support guidance set forth in section 4.4.1.3 of this policy. JIS connected computers will be configured in such a way that court users cannot change or disable this setting.

4.1.6.1 Password Locked Screensavers provide a critical safeguard and may not be disabled. However, in certain instances where business practices are sufficiently impacted, the 15 minute time limit may be extended. The AOC ISD Director will consider such extension requests on a case-by-case basis, and make the final determination after performing a thorough business impact and security analysis.

4.1.7 Reporting Misuse

Any JIS user who suspects misuse of his/her user account or workstation shall report such incidents to the JIS Site Coordinator. Site Coordinators shall report such incidents to AOC Customer Services.

4.1.8 Confidentiality Agreements

An employee of a court or county clerk's office may access the JIS only if he or she has signed a confidentiality agreement in a form approved by the AOC. Employees of courts or county clerks' offices shall review the confidentiality agreement annually.

4.1.9 Access by Vendors, Contractors, and Staff of Local Information Technology Departments

Vendors, contractors, and staff of local information technology departments may be granted security privileges for access to non-public data in the JIS if such access is needed in order to develop or maintain an information system for a court or the AOC. Such access shall be governed by written agreements between the AOC, the court or county clerk, and the vendor, contractor, or local information technology department. Such contracts shall require the employees of the vendor, contractor, or local information technology department to sign a confidentiality agreement, and for the court or county clerk to keep the signed copies and to certify to the AOC that such agreements have been executed.

5. ON-LINE AND OTHER SERVICES

5.3 The Extranet (Inside.Courts.Wa.Gov)

5.3.1 Access to the extranet is restricted to judicial officers, county clerks and their staffs, court employees, and other employees of the judicial branch.

5.3.2 Access to the extranet may be granted by the AOC Information Services Director on a temporary basis to city and county information technology department employees, or others in local government if it is necessary to perform services for the judicial branch or a court.

5.4 Data Warehouse

COMMENT

The data warehouse is a central repository of court data. Court data is uploaded nightly to the JIS data warehouse.

5.4.1 In all cases governed by Section 5.5, access will be appropriate to the user's case level security.

5.4.2 Courts and county clerks will be granted access to the JIS data warehouse using AOC supplied and maintained query software.

5.4.3 Requests for access to additional data elements must be submitted to AOC Customer Services

6. USE OF CUSTOMER SERVICES

6.1 AOC Customer Services provides assistance to courts, county clerks, criminal justice and other public agency users. It does not provide assistance to third-party clients of JIS-Link subscribers and does not provide phone training in the JIS-Link application.

6.2 Only designated users may place calls to Customer Services. Designated users include judicial officers, county clerks, court administrators, and site coordinators, and court staff who are designated by their administrator as authorized callers.