OVERVIEW OF PUBLIC PORTAL ACCESS ROLES AND APPROVAL PROCEDURES

MOU-BASED ACCESS

- Portal roles designed for agencies with MOUS will be secure roles, meaning that users will not be able to select and request the actual desired roles; only a Portal administrator (i.e. RIS approvers) can administratively assign the role to a user.
- Agencies seeking to register staff for elevated access based on MOUs will need to submit a list of authorized users with names and email addresses. This should be done as soon as possible for a complete list of all current users (agencies should be made to understand that staff who were previously registered on the legacy public access sites will not be automatically re-enrolled in the new system, but must re-register).
- Agencies should also designate one or more authorized agency contacts who can verify requests if questions arise, and who will be responsible for updating the Helpdesk anytime a new user's access is to be added or an existing user's access is to be terminated. They should be instructed to submit these communications as needed to the Helpdesk.
- RIS personnel should maintain an electronic folder for lists of users by agency/organization, and keep it updated as needed. Periodic audits in collaboration with the agencies might also be helpful.
- All Portal access requests from agency personnel based on MOUs will be made using a generic agency access request. Requestors must first self-register their accounts on the Portal in the standard way, then follow the "request access" process to select the role of "Agency/Justice Partner Access". *Important: this is a "gatekeeping" role that is not connected to any actual elevated access to any cases. It is necessary because there are varying levels of MOU-based access that are not all specific to only one agency (and more likely to be built in the future), and it would likely cause confusion and errors for external agencies to have to select the correct role from among many similar ones. Approvers will need to approve this access request when appropriate, then open that user's registration and administratively assign the correct MOU-based access role (see definitions of roles below).*
- Approvers should verify access requests by consulting lists of approved users submitted by agencies (bullets #2-4 above), and approve requests based on matching the requestor to an authorized user on the list. If the user is not found on the list, the request can be denied and/or the approver can contact the agency contact person for verification.
- After approving an access request for the "Agency/Justice Partner" role, the approved should then go to "Manage Users", find and open up that newly-

approved user, and, from the "role" dropdown menu, administratively assign the appropriate secure role based on the user's agency or organization.

- The MOU-based roles currently available[1] are:

  - AGENCY ACCESS– CR: This role gives access to all public (public limited case security) Criminal Division cases. As per existing MOUS, it is the appropriate role for these agencies:
    - Community Justice Center, DOC, Sentencing Commissioner, VCIC, and VRU, police departments, AGO, CRG, Court's law enforcement view, DEA, DPS, DPS, Disciplinary Counsel, Pretrial Services, ICE, US Probation, ATF, F&W, VT Forensics, VLA, Vt Assoc of Ct Diversion, DMV, Liquor and Lottery, Sec of State.

  - AGENCY ACCESS – CRFAM: This role gives access to all public (public limited case security) criminal and family cases (Domestic and RFA) as well as juvenile cases (juvenile confidential case security). As per existing MOUs it is the appropriate role for these agencies:
    - CDD, Diversion, DAIL, DefGen, DCF-FSD, and OCS, VCJR, and for the "JUD-Partner" role for VCAS.

  - SAO: This role is for state's attorneys and state's attorney's office authorized staff (SAO administrative staff should register with this role rather than the generic non-secure "legal admin" role). It provides access to all public (public limited case security) criminal cases as well as all juvenile (juvenile confidential case security) cases. It does not grant access to domestic, RFA, probate or other dockets.

OTHER SUPERIOR COURT ROLES (NON-MOU)

The access roles listed below are not MOU-based, but rather are based on the requestor's status as a party or participant in particular cases. Users' Portal accounts are linked by RIS approvers to their Odyssey entity record number, so that the user gets access (generally)[2] to all cases in which he or she is involved.

---

[1] *NOTE: Currently there are active Portal roles for DMV and Diversion being used by those agencies' staff for judicial bureau cases. Since these access roles are MOU-based as well, it is recommended that they be made secure roles as well and follow the same approval procedure going forward as outlined above. However, the existing Diversion role is likely now obsolete since diversion staff would have greater access under the CRFAM role above. Some communication with Diversion management would be warranted to facilitate this transition; existing Diversion Portal users could be administratively granted the CRFAM right if it is confirmed that all should receive it.

[2] One exception is for parties in juvenile cases, who cannot be granted remote elevated access to their cases, but must view them at a courthouse with a judge's prior permission.

- CASE PARTY: This role is for litigants in most case types. It grants access to all public (public and public limited case security) and confidential case information in the person's own case. A case party may generally register for elevated access to his or her own case(s) regardless of whether he or she is represented by an attorney. Access approval is a one time process; after the party's portal account is linked to his or her Odyssey entity, elevated access will transfer to all other cases in which he or she is a party (aside from juvenile cases).
    - *IMPORTANT: To grant Case Party access, approvers must go into the requestor's case in Odyssey (identified as part of the required request submission) and verify the requestor's identify from either (1) the person's Notice of Pro Se Appearance listing their name and email address, or (2) an "eServices Request Form" filed by the person into the case (also listing their name and the email address under which they wish to register). This verification from one of these forms is a prerequisite for granting access; where such a document is not found in the case record, the request should be denied with instructions to file the form into the case and then resubmit the access request. Note: parties should NOT send either of these case documents directly to the Helpdesk- they must be filed at the courthouse.*

- ATTORNEY: This role functions similarly to the Case Party role by linking the attorney's portal account to the attorney's Odyssey entity, giving the user access to all cases (public, public limited, confidential and juvenile confidential) in which the attorney is counsel of record. Attorneys' email addresses are generally all on record in the system already; matching up the bar number and the email address should be sufficient verification. If an attorney seeks to register with an email address different than one on record, the request could be denied and/or further verification could be requested.

- LEGAL ADMIN: This role is for legal support staff in firms and organizations who are authorized to access case information on behalf of the attorneys with whom they work. Although this is not an MOU-based role, it may make sense to follow a similar procedure for approvals as those roles (a manager or administrative contact person submits and maintains a list of authorized users). Because legal support staff are not entered as parties or attorneys in Odyssey, users granted this role are linked to the Odyssey attorney entities for whom they work (can specified in access request and/or through submission of preapproved list).

- GAL: This role is for Guardians Ad Litem. It functions similar to the Case Party role except that it does allow elevated access to juvenile cases. GALs may submit an eServices request form (and/or access could be done

administratively based on requests from the statewide or regional Judiciary GAL program managers).

- LAW ENFORCEMENT OFFICER: This role is for law enforcement officers to access their own Judicial Bureau ticket cases and to enter scheduling information for Judicial Bureau hearings. It does not grant any access to criminal or other Superior Court cases.

- LAW ENFORCEMENT ADMIN: This role is for law enforcement agency administrators and supervisors responsible for entering scheduling information for multiple officers within the agency.

**KIOSK ROLE: This secure role is used related to public access at courthouse access terminals. RIS approvers should not have to interact with this role in any way.*