

SECTION VII | LOOKUP TABLE

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
User Role 1 Judges and authorized court and clerk's office personnel	All court records, except those expunged pursuant to s. 943.0585, F.S., with discretionary limits based on local security policy. Each court and clerk must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in performance of their official duties. Access to records sealed pursuant to s. 943.059(4), F.S., is permitted for judges to assist in performance of case-related adjudicatory responsibilities.	In-house secure network and secure web access.
User Role 2 Florida State Attorneys' Offices and the Office of Statewide Prosecution	All records except those that are expunged or sealed, or, unless Level B access is assigned to this role in the Access Security Matrix, those records automatically confidential under rule 2.420(d)(1) Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order. Access to Social Security numbers by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to HIV test results as permitted by §381.004(5)(c), F.S. Access to sexually transmitted disease results as permitted by s. 384.29(1), F.S.	Secure access through user name and password by written notarized agreement. Agency gatekeeper is responsible for maintaining authorized user list. Each agency must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in performance of their official duties.

	Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5, F.S. Access to mental health records as permitted by §§ 394.4615(3)(b), 394.4655(3)4)(c), and F.S. Access to identities of victims of sexual and child abuse when originating from law enforcement as permitted by s. 119.0714(1)(h), F.S. Access to children and families in need of services records as permitted by s.984.06(3), F.S. Access to juvenile records as permitted by §§39.0132(4)(a)(1) and 985.04(1)(b), F.S.	
User Role 3 Attorneys of record	All records except those that are expunged or sealed; access may be denied to records or information automatically confidential under rule 2.420(d)(1) Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order, depending upon the type of case and the language of the court order. Access will be changed to Registered User when the attorney's appearance is terminated in accordance with rule 2.505, Fla. R. Gen. Prac. & Jud. Admin..	Secure access through user name and password by written notarized agreement. The gatekeeper is responsible for maintaining authorized user list.
User Role 4 Parties	All records in the party's case except those that are expunged or sealed; access may be denied to information automatically confidential under rule 2.420(d)(1), or made confidential by court	Secure access on case-by-case basis. Access by notarized request to insure identity of party.

	order, depending upon case type and the language of the order.	
User Role 5 Public in Clerks' offices and Registered Users	All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1) Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order. Viewable on request remote access to images of records in cases governed by the Florida Family Law Rules of Procedure, Florida Rules of Juvenile Procedure, or Florida Probate Rules, pursuant to §28.2221(5)(a), F.S.	Secure access through user name and password or in person at Clerks' offices.
User Role 6 General government and constitutional officers	All records except those that are expunged or sealed, or, unless Level "B" access is assigned to this role in the Access Security Matrix, those records automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order. Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S.	Secure access through username and password by written notarized agreement. The Agency gatekeeper is responsible for maintaining authorized user list. Each agency must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties.
User Role 7 General public (without registration agreement)	All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), Fla. R. Gen. Prac. & Jud. Admin. or made confidential by court order. No remote access to images of records in cases governed by the Florida Family Law Rules of Procedure, Florida Rules of Juvenile Procedure, or Florida	None. Anonymous web-based access permitted.

	Probate Rules, pursuant to §28.2221(5)(a), F.S.	
User Role 8 Certified law enforcement officers of federal and Florida state and local law enforcement agencies, Florida Department of Corrections, and the Florida Department of Law Enforcement	All records except those that are expunged or sealed, or, unless Level “B” access is assigned to this role in the Access Security Matrix, those records automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order. Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to HIV test results as permitted by §§381.004(2)(e), and 951.27 F.S. Access to sexually transmitted disease results as permitted by §384.29(1), F.S. Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5., F.S. Access to identities of victims of sexual and child abuse when originating from law enforcement as permitted by §119.0714(1)(h), F.S. Access to children and families in need of services records as permitted by §984.06(3), F.S. Access to juvenile records as permitted by §§39.0132(4)(a)(1) and 985.04(1)(b), F.S.	Secure access through username and password by written notarized agreement. The agency gatekeeper is responsible for maintaining an authorized user list. Each agency must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties.

User Role 9 Florida Attorney General's Office and the Florida Department of Children and Families	All records except those that are expunged or sealed, or, unless Level "B" access is assigned to this role in the Access Security Matrix, those records automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order. Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5., F.S. Access to children and families in need of services records as permitted by §984.06(3), F.S. Access to juvenile records as permitted by §§39.0132(4)(a)(1) and 985.04(1)(b), F.S.	Secure access through username and password by written notarized agreement. The agency gatekeeper is responsible for maintaining authorized user list. Each agency must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties.
User Role 10 Florida School Districts (Truancy)	All records except those that are expunged or sealed, or, unless Level "B" access is assigned to this role in the Access Security Matrix, those records automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order. Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to juvenile delinquency records as permitted by §985.04(1)(b), F.S.	Secure access through username and password by written notarized agreement. Agency gatekeeper is responsible for maintaining authorized user list. Each school district must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties.

User Role 11 Commercial purchasers of bulk records	All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order. No remote access to images of records in cases governed by the Florida Family Law Rules of Procedure, Florida Rules of Juvenile Procedure, or Florida Probate Rules, pursuant to s. 28.2221(5)(a), F.S.	Secure access through username and password by written notarized agreement. The commercial purchaser gatekeeper is responsible for maintaining an authorized user list.
User Role 12 Florida Office of the Public Defender (Institutional Access only)	All records except those that are expunged or sealed; or, unless Level “B” access is assigned in the Access Security matrix, access may be denied to records or information automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order, depending upon the type of case and the language of the court order. The Office of the Public Defender is considered the attorney of record at a defendant’s first appearance as permitted by §985.045(2) and rules 8.010 and 8.165, Fla. R. Juv. P. for juvenile defendants and §27.51 and rule 3.130, la. R. Crim. P. for adult defendants. Access will be changed to User Role 6 when the public defender is no longer the attorney of record or another attorney is assigned.	Secure access through username and password by written notarized agreement. The gatekeeper is responsible for maintaining authorized user list. Each public defender must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties.
User Role 13 Office of Criminal Conflict and Civil Regional Counsel (Institutional Access only)	All records except those that are expunged or sealed; or, unless Level “B” access is assigned to this role in the	Secure access through username and password by written notarized agreement. The gatekeeper is responsible



	Access Security Matrix, access may be denied to records or information automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order, depending upon the type of case and the language of the court order. The Office of Criminal Conflict and Civil Regional Counsel (OCCRC) is considered the attorney of record at a party's first appearance in civil proceedings listed in §27.511(6), F.S., and in criminal proceedings is entitled to appointment as attorney of record upon the Public Defender's declaration of conflict in case types listed in §27.511(5), F.S. Access will be changed to User Role 6 when the OCCRC is no longer the attorney of record or another attorney is assigned.	for maintaining authorized user list. Each regional counsel must establish written policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties,
User Role 14 Statewide Guardian ad Litem Office	All records except those that are expunged or sealed, or, unless Level "B" access is assigned to this role in the Access Security Matrix, automatically confidential under rule 2.420(d)(1), Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order. Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S.	Secure access through username and password by written notarized agreement. The gatekeeper is responsible for maintaining authorized user list. Each guardian ad litem must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties.

	Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5., F.S. Access to children and families in need of services records as permitted by §984.06(3), F.S. Access to juvenile records as permitted by §§39.0132(4)(a)(1) and 985.04(1)(b), F.S. Access for guardian ad litem appointed as permitted by §39.822, F.S.	
User Role 15 Justice Administrative Commission	All records except those that are expunged or sealed; or, unless Level “B” access is assigned to this role in the Access Security Matrix, access may be denied to records or information automatically confidential under rule 2.420(d)(1), Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order, depending upon the type of case and the language of the court order. Access to Social Security numbers by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to HIV test results as permitted by §381.004(5)(c), F.S. Access to sexually transmitted disease results as permitted by §384.29(1), F.S. Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5, F.S.	Secure access through username and password by written notarized agreement. The gatekeeper is responsible for maintaining authorized user list. The justice administrative commission must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties.

	Access to mental health records as permitted by §§394.4615(3)(b), 394.4655(3)4(c), and F.S. Access to identities of victims of sexual and child abuse when originating from law enforcement as permitted by §119.0714(1)(h), F.S. Access to children and families in need of services records as permitted by §984.06(3), F.S. Access to juvenile records as permitted by §§39.0132(4)(a)(1) and 985.04(1)(b), F.S.	
--	--	--

