DAKOTA COUNTY ATTORNEY'S OFFICE
DATA CONFIDENTIALITY AND USER SECURITY AGREEMENT

PURPOSE OF AGREEMENT

Dakota County Attorney's Office staff, volunteers and interns whose assignments reasonably require access to County Attorney Office and client data are authorized to access data and electronic database systems through the County Attorney's Office depending on each individual's business-related functions and responsibilities. **A business-related function and responsibility means that the individual has a requirement, duty or obligation for the efficient performance of governmental tasks or responsibilities and as required or authorized by law or court rule in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State or local court or agency or before any self-regulatory board.**

The data you have access to include data classified by the Minnesota Government Data Practices Act (MGDPA), Minn. Stat.Ch. 13, as private and confidential data on individuals as well as nonpublic data and protected nonpublic data not on individuals (e.g. corporations, government entities) regarding offenders, victims, witnesses, County staff and clients, and others through the work of the County Attorney's Office. In addition to the MGDPA, there are other state and federal privacy laws, rules of court and professional responsibility, and system security and use policies that protect the data and provide for penalties for misuse. Dakota County and the County Attorney's Office also have policies governing the integrity and security of private and confidential client and business data:

- Dakota County Policy 1013 Data Practices
- Dakota County Policy 3500 HIPAA (Health Insurance Portability and Accountability Act)
- Dakota County Policy 6001 Acceptable Use of Technology Resources
- Dakota County Policy 6003 Email Management
- Dakota County Policy 6004 Information Security
- Dakota County Policy 6005 Records Retention, Disposition and Litigation Holds
- Dakota County Policy 6007 Mobile Devices
- Dakota County Attorney's Office Communications Policy
- Dakota County Attorney's Office Social Media Policy

It is your responsibility to be familiar with and in compliance with the laws and policies governing the data and electronic database systems you have a legitimate need to access to perform your work functions. If you need clarification, training or guidance concerning the proper access, use or dissemination of data or electronic database systems, contact your supervisor. Dakota County and the County Attorney's Office have training materials and on-going training sessions available for employees.

GUIDELINES

The following guidelines governing access, dissemination, and security of data and electronic database systems are not intended to be exclusive and are in addition to regulation of the data as stated herein:

- Only appropriate business-related searches are permitted. For example, you cannot use an electronic database system to look up information about family members, acquaintances, or out of personal curiosity.

- Disclosure or sharing of data is only permitted to others whose work assignments reasonably require access to the data and only as authorized by law, by court order, or by informed consent of the data subject.

- Passwords, logins, access codes, and security questions/answers may not be shared with others. If you forgot your access information, contact the Dakota County Help Desk or the County Attorney's Office system administrator.

- Sign off systems or use a locked screensaver when leaving the workstation/computing device. It is the employee's responsibility to ensure that data on the device is not viewed by others who do not have a permissible purpose to view the data.

- Many electronic database systems conduct regular user and system audits for adherence to use and security policies. Penalties for misuse of access, dissemination, and security of data can include loss of the system for the entire County Attorney's Office, sometimes without advance notice to the County Attorney's Office or the individual violator.

- There is no expectation of privacy with regard to any use of the system or data contained on the portion of a device that is used for business purposes.

- Access of systems outside the Dakota County network must comply with all Dakota County IT policies. Portable devices must utilize appropriate encryption methods and security tools approved by IT to protect the data from unauthorized access. Adherence to County Policy 6007 governing Mobile Devices is required of all employees.

- Immediately report to a supervisor breaches or compromises of private and/or confidential data or access to a system by an unauthorized person.

COMPLIANCE/VIOLATIONS

The County Attorney's Office will verify compliance with this Agreement through various methods, including, but not limited to, business tools, random internal and external audits, and supervisory review. Failure to comply with the terms of this Agreement, including the guidelines herein, as well as federal and state privacy and security laws, Dakota County policies, and system security policies/agreements could result in termination of individual and/or Dakota County privileges to the data/system. Violations could result in an employee disciplinary action up to and including termination from employment or, as appropriate, volunteer or internship position, and/or legal action against the individual employee, volunteer, or intern. Willful or knowing violations may be illegal and carry the possibility of criminal penalties. Additionally, violations of security requirements of certain databases may subject the violator to civil causes of action.

ACKNOWLEDGEMENT

By signing below I acknowledge that I understand and agree to abide by the terms contained in this Agreement, including the guidelines, and all relevant statutes, rules, regulations, policies and procedures governing the data and data systems I have access to during the course of my employment, internship or volunteering with the County Attorney's Office. I also agree that I will immediately report to my supervisor any violation or potential violation, whether intentional or not, of this Agreement.

Printed Name _____ Date _____

Signature _____

The original signed Agreement will be retained in the employee's file and a copy given to the employee.