MDC User Security Agreement

Representing the Kenton County Emergency Communications Center, and Kenton Police

The challenges of building a secure, wireless data network for use by public safety forces are numerous. It cannot be stressed enough that strict adherence to the safeguards built into this system be adhered to. Each Mobile Data Computer (MDC) user must read and sign this User Security Agreement. This signed agreement becomes part of the permanent files stored at the Kenton County Emergency Communications Center (hereafter referred to as KCECC). Violation of any part of this agreement could result in various penalties, up to and including removal of the MDC from the users' vehicle. Your signature on this agreement indicates that you have read and understand the serious security issues listed, and that you are pledging to abide by them during your participation in the Mobile Data Program.

Kenton County Emergency Communications Center provides the following software on MDCs:

- Law Enforcement Mobile for communications and dispatch
- Law Enforcement Record Management System (LERMS) for case management records access
- Netmotion for secure connection to CAD system
- KYOPS

Each Mobile Data Network participant has been advised and understands:

- MDC's are secured using 2-part authentication.
    - Part 1 is by the use of a token device, currently a "Yubikey".
    - Part 2 is by the use of a user assigned password for specific data connections or software logins
- Each user has a unique password and login that is valid for the software above (with exception for KYOPS which is maintained through KSP).
    - Passwords must be be 8-15 characters in length, contain at least 1 number and 1 letter.
    - Passwords should NOT be recognizable words found in the dictionary.
    - Passwords are encouraged to use mixed alpha and numeric characters
    - Passwords are required to be changed at least every 60 days.
    - Passwords cannot be reused for 10 iterations.
- No user shall share a user ID or password to gain access to the Mobile Data Network.
- Each user is responsible for the integrity of the Mobile Data Computer.
- Physical security of the MDC is very important.
    - The device should remain under the user's control at all times.
    - The device should only be removed from the vehicle for authorized purposes.
    - Remove the device if the vehicle is to be services by non-agency personnel.
    - Physically store the device under your direct control at all times.

    - Bring the device to the KCECC if your department is unable to provide long-term, secure storage.
    - If the user is not in the vehicle or within close proximity then the vehicle must be locked when the MDC is inside.
- Only Kenton County Technology Services Staff may affect repairs or adjustments to the Mobile Data Computers.
    - Do not take the device to any computer repair shop for service.
    - Only Kenton County Technology Services personnel can authorize exceptions.
    - Damage to the MDC or issues with software shall be reported immediately to Kenton County Technology Services staff by emailing kentoncountytickets@cforward.com.
- All "Inquiry" users of the Mobile Data Network must be LINK/NCIC certified.
    - Each user's certification must be active and up to date.
    - ~~e~~ If certification lapses, the Inquiry function privilege will be de-activated
    - Inquiry privileges will be re-activated once proper re-certification is obtained.
    - Records of all LINK/NCIC certifications will be maintained by each department.
- All transactions by a Mobile Data Computer are logged and recorded by the system.
    - The system's server maintains a database of all transactions.
    - This includes all inquiries, messages, and CAD/RMS information.
    - All transactions and reports are available to the System Administrator(s).
    - All transactions are subject to Open Records Requests.
    - These transaction reports are available for a minimum of one (1) year.
- Playing games of any kind on the MDC is prohibited
- Defacing or personalizing MDCs in any way, including the placement of decals, stickers, or writing, by any entity other than Kenton County Technology Services, is prohibited

Please note that safeguards are deemed necessary to protect the integrity of the information shared across the Mobile Data network through the use on an MDC device. It is critical that we all share the responsibility of protecting this information. We also need to work together to help ensure the safety and security of the large physical investment in hardware and software. The security provisions of existing contracts with the supervising authority of LINK/NCIC also bind us.

User's Signature _____ Date _____

Print Full Name _____ Agency _____