Unified Infrastructure/Organization Computer System/Software Use Policy

1. Statement of Responsibility

All employees are charged with the security and integrity of the computer system. Employees are asked to help maintain the files and hardware that comprise the system safe from harm.

2. Definitions:

Unified Organization – Combine City, County, outlying agency employees and building, departments, etc. supported by Goshen County IT.
Unified Infrastructure – Combined network, server, PC, Laptop, wireless, network components

3. Statement of Compliance

By using any part or device of the Unified network you are showing your compliance and understanding of this policy.

4. Statement of Liability

Individuals granted accesses to the Unified systems are held liable for improper dissemination of sensitive data, even after termination of employment. The employee may be subject to criminal and civil penalties.

5. Policy Changes

This policy is subject to change without notice. It is the responsibility of the Unified Organization employee to inform him/herself of changes to this policy.

6. Ownership of Work

E-mail, computer, internet, and voice mail systems are the property of Unified infrastructure. Anything created, loaded, or accessed on these systems becomes the property of the Unified Organization. Employees have no privacy rights to the content of e-mail messages or data files, and the Unified Organization has the right to review, monitor, audit, intercept, copy, download, and disclose any communications or files created or maintained on information systems at any time, without prior notice.

7. Physical Security

Only authorized Unified Organization personnel may use the Unified Infrastructure computers. Moving, connecting or disconnecting equipment is to be done by the Goshen County Information Technology Department.

8. Encryption

Materials of a sensitive nature or which constitute Unified Organization confidential information shall not be sent out by the internet unless the information is appropriately encrypted to prevent interception by third parties.

9. Authorized Use

Use of the Unified Infrastructure for non-employment purposes may result in discipline and/or monitory charge.

10. Authorized Access

Unified Organization employees will be given explicit access to programs, files, and resources needed to perform their assigned duties. Attempted access to programs, files, or resources to which the employee has not been given permission to utilize will make the employee subject to disciplinary action.

11. Departmental Barrier

Departmental data will remain under the control of the department. No access to department generated data by any other department will be allowed without the permission of the respective department head.

12. Programs

Only authorized and licensed programs may be installed and used on Unified Infrastructure computers. All programs must be installed at the direction of the Goshen County Information Technology Department.

13. Copyright

No material which violates copyright law may be installed, stored, or used on Unified Infrastructure computers, and no Unified Infrastructure computer may be used in the creation or distribution of said material. Items include, and are not limited to:

- Unlicensed software

- Digital music (MP3's, WMA's, CD's)
- Digital video (DVD's MPEG2/4)

14. E-Mail

Every Unified Organization employee will be assigned an e-mail address. This address can be used from any work station in the county, or externally. This e-mail account will be deleted upon the termination of the employee. All employees must use the following guidelines for e-mail access:

- The employee will not allow anyone besides him/herself to access his/her account
- The employee will not engage in mass-mailing (spamming) with their e-mail account
- The employee's email is subject to inspection and monitoring by commanding officers and Information Technology
- The e-mail account is subject to virus and spam filtration

15. Internet

Every computer located within the facilities of the Unified Organization has been given access to the internet. All authorized persons are able to access the internet from these computers given that the following rules are followed:

- Unless in the act of investigating or researching an assigned case, no one will be allowed to knowingly access sites which contain social networking, pornography, hate or anti-government organizations, or anything unbecoming of an officer or employee which could have adverse affects on personnel moral or public reputation.
- No one will download, install, or access any subversive files or programs. IE: Viruses, Trojan horses, Spy ware, Ad ware
- No one will attempt to access another computer system without permission (hacking/cracking)
- All Unified Organization and infrastructure activity will be recorded including email, internet, network access
- Internet access for users or computers is subject to revocation by the decision of department heads or the Goshen County Information Technology department.
- Internet access to specified sites, or class of sites, or types of media is subject to filtration by the decision of department heads or Information Technology

16. Network Access

1. Logon and password

Every Unified Organization employee will be assigned a network logon which will be deactivated upon termination of employment. This logon can be used at any similarly classed Unified Organization department (IE, Law enforcement and government). The employee is to use their personal access their e-mail and files. The employee is responsible for all activity on Unified Infrastructure under

his/her logon ID. Special station accounts (booking, control) are created for multi-person locations. These logons are to be used for those purposes only.

2. Network Storage

Every employee will be allowed to store files on the network. They will be assigned a private storage place, and have access to a common storage. Employees will not attempt to access other employee's personal storage without permission. Employees will not destroy, damage, or deface files in the common storage area.

3. Unauthorized Access/Use

Any unauthorized access to or of another member's logon or file(s) is absolutely prohibited. Employees who utilize software applications under another employee logon identity or access individual file(s) without permission will be subject to disciplinary action.

4. Resource Utilization

No user will utilize network resources (Internet, E-Mail, Storage, Printers, et al.) in a manner in which that use becomes an undue drain on the capacity of the system (i.e. streaming video, music, etc)

17. Remote Access

Remote access into Unified Infrastructure computer systems will be done by encrypted means. All remote activity will be logged and secured by username and password authentication.

18. Notice of Status Change

It is the responsibility of the Unified Organization department heads to inform Information Technology of an employee status change so that the employee's status can be reflected in their assigned logon. These status changes are:

- Hire
- Termination
- Extended leave

19. Data Disposal

Devices containing sensitive data are to be completely deleted, overwritten or destroyed before leaving the control of trusted users.

20. Workstation Retire

All computers that are replaced will have their hard drives completely erased and overwritten to ensure no data leakage. Computers from sensitive environments will have their hard drives erased, overwritten, and destroyed.