



Buildings & Grounds Committee

Committee Meeting

60 Central Ave.
Cortland, NY 13045
<http://www.cortland-co.org>

~ Minutes ~

Tuesday, April 11, 2023

10:00 AM

Room B20

CALL TO ORDER

The meeting was called to order at 10:00 AM by Committee Chair Paul Heider

Attendee Name	Organization	Title	Status	Arrived
Douglas Bentley	Cortland County, NY	Committee Member	Present	
Beau Harbin	Cortland County, NY	Committee Member	Present	
Ronald J. Van Dee	Cortland County, NY	Committee Member	Present	
Ann Homer	Cortland County, NY	Committee Member	Excused	
Paul Heider	Cortland County, NY	Committee Chair	Present	
Joseph Nauseef	Cortland County, NY	Committee Member	Present	
Eugene Waldbauer	Cortland County, NY	Committee Vice Chair	Present	
Kevin Fitch	Cortland County, NY	Chair of the Legislature	Present	
Rob Corpora	Cortland County, NY	County Administrator	Present	
Savannah Hempstead	Cortland County, NY	Clerk of the Legislature	Present	
Charles Miller	Cortland County, NY	Superintendent Buildings and Grounds	Present	
Allen Pankhurst	Cortland County, NY	Building Maintenance Mechanic	Present	
Andrea Piedigrossi	Cortland Youth Bureau	Director	Present	
George Wagner	Cortland County, NY	Board Member	Present	
Christopher Newell	Cortland County, NY	Board Member	Present	
Thomas McGrath	Cortland County, NY	Deputy Director, Information Technology	Present	
Jack Hess	Cortland County, NY	Director, Information Technology	Present	
Melanie Vilardi	Cortland County, NY	Deputy County Administrator	Present	
Andrea Herzog	Cortland County, NY	Director of Finance	Present	
Heather Johnson	Cortland Youth Bureau	Youth Services Supervisor	Present	
Margaret Mellot	Cortland Standard	Reporter	Remote	

MINUTES

1. Buildings & Grounds Committee - Committee Meeting - Mar 7, 2023 10:00 AM

RESULT:	APPROVED [UNANIMOUS]
MOVER:	Ronald J. Van Dee, Committee Member
SECONDER:	Joseph Nauseef, Committee Member
AYES:	Bentley, Harbin, Van Dee, Heider, Nauseef, Waldbauer
EXCUSED:	Ann Homer

DISCUSSION ITEMS

1. County Office Building Gymnasium Use - Andrea Piedigrossi, Cortland Youth Bureau Director

RESULT:	COMPLETED
----------------	------------------

2. Courthouse Project Funding

RESULT:	COMPLETED
----------------	------------------

3. 22 West Court Street Update

RESULT:	COMPLETED
----------------	------------------

4. Cortland County Employee Info Security Policy

RESULT:	COMPLETED
----------------	------------------

RESOLUTIONS

AGENDA ITEM NO. 1 – Authorize Agreement with Bell & Spina Architects for Specs for Cortland County Courthouse Dome/Cupola Rehabilitation - Buildings and Grounds Department

RESULT:	APPROVED [UNANIMOUS]
	Next: 4/18/2023 10:00 AM
MOVER:	Ronald J. Van Dee, Committee Member
SECONDER:	Beau Harbin, Committee Member
AYES:	Bentley, Harbin, Van Dee, Heider, Nauseef, Waldbauer
EXCUSED:	Ann Homer

ON MOTION OF HEIDER

RESOLUTION NO.

Authorize Agreement with Bell & Spina Architects for Specs for Cortland County Courthouse Dome/Cupola Rehabilitation - Buildings and Grounds Department

WHEREAS, the County was awarded a grant from the Dormitory Authority of the State of New York (DASNY) in the amount of \$2,396,000 for the restoration and preservation of the Cortland County Courthouse, AND

WHEREAS, the projects to be completed with this funding are the main entryway and the dome/cupola of the Cortland County Courthouse, AND

WHEREAS, to proceed with the dome/cupola project, there is a need to have engineering specifications drawn up, AND

WHEREAS, Bell & Spina Architects of 215 Wyoming Street Syracuse, NY 13204, has the expertise to draw up specifications for said projects, AND

WHEREAS, Resolution No. 70-22 authorized the allocation of \$1,000,000 of American Rescue Plan funding for the planning, preparation and implementation of repairs to the Cortland County Courthouse and the funding is available in Account No. A16205.52320.ARP, NOW THEREFORE BE IT

RESOLVED, that the County Administrator, upon approval of the County Attorney, or their designee, is hereby authorized and directed to execute a contract, for an amount not to exceed \$200,000, with Bell & Spina Architects, 215 Wyoming Street Syracuse, NY 13204, for the completion of the specifications for said project, AND BE IT FURTHER

RESOLVED, that the County Administrator, upon review and approval by the County Attorney or designee and subject to appropriation of funding, be and hereby is authorized to enter into an agreement with Bell & Spina Architects of 215 Wyoming Street Syracuse, NY 13204, for said purposes at a cost not to exceed \$200,000 to be paid from Account No. A16205.52320.ARP.

ACTION ITEMS

1. Approve Use of County Property for 2023 Pumpkinfest

RESULT:	APPROVED [UNANIMOUS]
MOVER:	Joseph Nauseef, Committee Member
SECONDER:	Beau Harbin, Committee Member
AYES:	Bentley, Harbin, Van Dee, Heider, Nauseef, Waldbauer
EXCUSED:	Ann Homer

MONTHLY REPORTS

1. IT Monthly Report

RESULT:	COMPLETED
----------------	------------------

2. Buildings & Grounds Activities and Time Line Reports

RESULT:	COMPLETED
----------------	------------------

ADJOURNMENT

The meeting was closed at 11:00 AM



Buildings & Grounds Committee

Committee Meeting

60 Central Ave.
Cortland, NY 13045
<http://www.cortland-co.org>

~ Minutes ~

Tuesday, March 7, 2023

10:00 AM

Room 302

CALL TO ORDER

The meeting was called to order at 10:00 AM by Committee Chair Paul Heider

Attendee Name	Organization	Title	Status	Arrived	Departed
Douglas Bentley	Cortland County, NY	Committee Member	Present		
Beau Harbin	Cortland County, NY	Committee Member	Present		
Ronald J. Van Dee	Cortland County, NY	Committee Member	Present		
Ann Homer	Cortland County, NY	Committee Member	Present		10:29 AM
Paul Heider	Cortland County, NY	Committee Chair	Present		
Joseph Nauseef	Cortland County, NY	Committee Member	Excused		
Eugene Waldbauer	Cortland County, NY	Committee Vice Chair	Present		
Rob Corpora	Cortland County, NY	County Administrator	Present		
Savannah Hempstead	Cortland County, NY	Clerk of the Legislature	Present		
Andrea Herzog	Cortland County, NY	Finance Director	Present		
Melanie Vilardi	Cortland County, NY	Deputy County Administrator	Present		
Charles Miller	Cortland County, NY	Superintendent Buildings and Grounds	Present		
Jack Hess	Cortland County, NY	Director, Information Technology	Present		
Scott Roman	Cortland County, NY	Director of Emergency Response and Communications	Present		
Thomas McGrath	Cortland County, NY	Deputy Director, Information Technology	Present		
Patricia Dawson	Cortland County, NY	Deputy Clerk of the Legislature	Remote		
Eddie Velazquez	Cortland Voice	Reporter	Remote		
Margaret Mellott	Cortland Standard	Reporter	Remote		
Kevin Fitch	Cortland County, NY	Chair of the Legislature	Remote		
George	Cortland	Board Member	Present	10:03	

Minutes Acceptance: Minutes of Mar 7, 2023 10:00 AM (MINUTES)

MINUTES

- Buildings & Grounds Committee - Committee Meeting - Feb 7, 2023 10:00 AM

RESULT:	APPROVED [UNANIMOUS]
MOVER:	Ann Homer, Committee Member
SECONDER:	Douglas Bentley, Committee Member
AYES:	Bentley, Harbin, Van Dee, Homer, Heider, Waldbauer
EXCUSED:	Joseph Nauseef

DISCUSSION ITEMS

- 22 West Court Street Update

RESULT:	COMPLETED
----------------	------------------

- Elevator at the County Office Building

RESULT:	COMPLETED
----------------	------------------

MONTHLY REPORTS

- IT Monthly Report

RESULT:	COMPLETED
----------------	------------------

- Buildings & Grounds Departmental Activities and Timelines

RESULT:	COMPLETED
----------------	------------------

RESOLUTIONS

Mr. VanDee MADE A MOTION to suspend the rules to entertain a resolution not on the agenda, Mr. Waldbauer SECONDED THE MOTION to suspend the rules; and upon voice vote of members present (Ms. Homer not present for vote), MOTION CARRIED.

AGENDA ITEM NO. 1 – Authorize Agreement with Bell & Spina Architects for Specs for Cortland County Courthouse Column and East/West Entrance Rehabilitation - Buildings and Grounds Department

RESULT:	APPROVED [5 TO 0]
	Next: 3/23/2023 6:00 PM
MOVER:	Ronald J. Van Dee, Committee Member
SECONDER:	Eugene Waldbauer, Committee Vice Chair
AYES:	Bentley, Harbin, Van Dee, Heider, Waldbauer
EXCUSED:	Joseph Nauseef
AWAY:	Ann Homer

ON MOTION OF HEIDER

RESOLUTION NO.

Authorize Agreement with Bell & Spina Architects for Specs for Cortland County Courthouse Column and East/West Entrance Rehabilitation - Buildings and Grounds Department

WHEREAS, the Cortland County Buildings and Grounds Committee recommends moving forward with necessary repairs and rehabilitation to the Cortland County Courthouse, AND

WHEREAS, the columns on the interior of the Courthouse and the east and west entrances of the

Courthouse are in need of repair and/or replacement, AND

WHEREAS, to proceed with the column and east/west entrance projects, there is a need to have engineering specifications drawn up, AND

WHEREAS, Bell & Spina Architects of 215 Wyoming Street Syracuse, NY 13204, has the expertise to draw up specifications for said projects, AND

WHEREAS, Resolution No. 70-22 authorized the allocation of \$1,000,000 of American Rescue Plan funding for the planning, preparation and implementation of repairs to the Cortland County Courthouse and the funding is available in Account No. A16205.52320.ARP, NOW THEREFORE BE IT

RESOLVED, that the County Administrator, upon approval of the County Attorney or designee, is hereby authorized and directed to execute a contract, for an amount not to exceed \$200,000, with Bell & Spina Architects, 215 Wyoming Street Syracuse, NY 13204, for the completion of the specifications for said projects, AND BE IT FURTHER

RESOLVED, that the County Administrator, upon review and approval by the County Attorney or designee and subject to appropriation of funding, be and hereby is authorized to enter into an agreement with Bell & Spina Architects of 215 Wyoming Street Syracuse, NY 13204, for said purposes at a cost not to exceed \$200,000, to be paid from Account No. A16205.52320.ARP.

ADJOURNMENT

The meeting was closed at 10:57 AM

22 West Court Street

Architect: King & King, Syracuse NY

April 2023

Updates

- Phase 4 interior construction
 - Construction has started with bi-weekly meetings
 - All trades on site and actively engaged
- IT - Fiber Optic connection, Syracuse Utilities engaged, Celerity engaged
- RFP out for IT equipment
- Vendor is being for networking design
- Motorola engaged for network work for radio system
- Generator arrival September 2023
- Additional exterior camera system equipment ordered
- Estimates received from state contractors for access control system
- Phase 5 bidding to be done in the next two months – site work to retaining wall, parking lot, sidewalks, drainage

Work completed

- Phase 1 - Interior demolition
- Phase 2 - Roof replacement
- Phase 3 - Window replacement

Future Work

- Phase 5 exterior site work – told architects to progress with bidding work
- Phase 6 site/security improvements

CORTLAND COUNTY
EMPLOYEE INFORMATION
 SECURITY POLICY



Release authorized by:
 The Cortland County
 Legislature

Adopted ~~6/24/2010~~

-Resolution

~~#192-10~~-Last Updated:

~~41/25/2018~~~~23~~

20~~23~~~~10~~ - 2018

Note: This is a condensation of the County's complete Information Security Policy. The numbering system of the complete document has been retained for reference purposes.

1. Purpose

Access to Cortland County's (hereinafter referred to as the County) information systems has been provided to all authorized County Entities¹, employees, consultants, contractors, interns, volunteers, and temporary workers (hereinafter referred to as "users") for the purpose of providing service to the residents of Cortland County. All users have a responsibility to maintain and protect the County's information assets against accidental or intentional disclosure or compromise. Each user also has the responsibility to maintain and protect the County's public image and to use the County's information systems in a legal/ethical manner consistent with County & department policies.

Information is essential to all services the County provides. As a result, information security is a critical factor in the delivery of County services. The integrity, availability, and confidentiality of County information collected, processed, and stored needs to be ensured. The accidental or intentional disclosure of non-public County information can have serious repercussions. The County, in the event its information resources are compromised due to user misconduct, can face legal liability associated with the disclosure of information governed by Federal and State Laws (e.g., Health Insurance Portability Accountability Act of 1996 (HIPAA)).

To ensure that the County's information resources are used in a responsible and productive manner, the following policy for using the County's information systems has been established.

- **Effective Date:** This policy is effective as of the date of issuance.
- **Expiration Date:** This policy remains in effect until superseded, amended, or canceled.

All use of information systems involves certain risks that must be addressed through proper controls. The protective requirements for each of the individual information systems within the County will vary according to the unique characteristics of the system, data sensitivity and mission-related criticality of the system or information. Appropriate levels of security and cost-effective controls, which are adequate to achieve an acceptable level of risk for each system, will be implemented through the guidance of this policy.

The policy ensures that all users are knowledgeable of acceptable behavior when using the County's information systems, understand their information security responsibilities and are held accountable.

Furthermore, the policy ensures that the County will protect and maintain the availability, integrity, confidentiality and non-repudiation of information and information resources.

1. **Availability:** This is the 'property' of being operational, accessible, functional and usable upon demand by an authorized entity, e.g., a system or a user.
2. **Integrity:** The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.
3. **Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities or processes.

¹ County Entity, for the purposes of this policy, shall include all County departments, offices, etc.

4. **Non-Repudiation:** The availability of irrefutable proof of:
 - a. the origin of data
 - b. the content integrity of data, and
 - c. the receipt and, optionally, the acceptance of data such that refutation of any of these is not possible.

Effective information security is a team effort involving all users who come in contact with information and information resources. In recognition of the need for teamwork, this policy clarifies responsibilities and duties associated with information security.

The policy aims to:

1. Establish an evolutionary, risk-managed information security program that defends against internal and external threats.
2. Establish a management structure that addresses the County's information security operation. Require that all users who use the County's information systems: a) be knowledgeable of acceptable County information system usage, b) understand their information security responsibilities, and c) be held accountable for their actions.

2. Scope

The policies contained in this document are applicable to all of the County's internal computer network (County Wide Area Network [WAN]), interconnections with systems outside the County WAN (e.g., Internet), and all other County information system resources, whether located within the physical confines of County property or at an off-site location. They cover all computer and communication devices (e.g., routers, modems, TDDs, radios, phones) owned or operated by the County. They also cover any computer or communications device ~~that is~~ that is present on County premises and connected to County information systems, but which may not be owned or operated by the County.

These policies are mandatory for all County organizational units, County Staff, and other authorized users having access to and/or using the information systems and resources of the County.

7. User Responsibilities

Users are responsible for adhering to policy and the security controls governing the security of the information resources under their control to prevent unauthorized disclosure of information.

Each user is responsible for the content of all text, audio and images that they place or send over email, voicemail, fax, the intranet or Internet. No abusive, profane or offensive language shall be transmitted through the County's systems. Users who wish to express personal opinions on the Internet are not to do so on the County's systems.

Information stored, processed and transmitted on the County's information systems are owned by the County, and, therefore, is a County resource in the custody of the user. It is the user's responsibility to ensure that all sensitive County information is adequately protected at all times – in the manner as prescribed by the user's department and County policy. When data is ~~transferred from~~ transferred from the user's custodial responsibility to another user, each user accepts the same responsibility of continued protection.

Users shall:

1. Protect others' privacy and confidentiality.
2. Consider organizational access before sending, filing, or destroying e-mail messages.
3. Remove messages, transient records, and reference copies in a timely manner.
4. Comply with department and unit/division policies, procedures, and standards.
5. Become cognizant of the sensitivity/criticality of the information they handle and apply appropriate protective measures when handling the information.
6. Coordinate the connection of Personal Communications Devices (PDAs) with the ~~County's Security Official (SO)~~ user's department head and the Information Technology Department (IT).
7. Coordinate the connection of devices with RF (radio frequency) capabilities (e.g., wireless access points, wireless LANs) with ~~the SO and~~ IT.
8. Not connect ~~a modem to a phone line while the same computer is connected to the County LAN non-County equipment to County information assets (computers, networking equipment, etc.)~~ without approval of ~~the SO and~~ the IT Department.
9. Use only software licensed to the County on County computers.
10. Use robust network passwords and change them as required. (Reference Section 22.7)
11. Never share ID or passwords with anyone else, including superiors and IT staff.
12. Never document passwords and put them on or near the computer (e.g., "sticky notes" under keyboards, on monitors, etc.) (Reference Section 22.7)
13. Log off or activate screensavers with password protection to protect the County's information when computers are left unattended. Automatic screensavers with password protection activate after 15 minutes of inactivity.
14. Never release non-public County information unless prior authorization from the department head has been obtained.
15. Not disclose sensitive County data to other County staff other than on a need-to-know basis.
16. Secure any physical copies of sensitive County data such as tapes, floppy disks, and printouts when left unattended.
17. Report indicators of virus infection and/or operational anomalies to IT personnel ~~or SO~~.
18. Report all discovered security vulnerabilities and/or computer security concerns to their supervisor and the SO and the IT Department.
19. When working at home, take reasonable measures consistent with workplace procedures to safeguard access to County information resources (e.g., computers, networks, data).
20. Never use the system for:
 - a) Activities unrelated to the County's mission; (See Section 10.1)
 - b) Activities unrelated to official assignments and/or job responsibilities; (See Section 10.1)
 - c) Any illegal purpose; (See Section 10.1)
 - d) The transmission of threatening, fraudulent, obscene or harassing materials or correspondence;
 - e) Unauthorized distribution of County or New York State data and information;
 - f) Interfering with or disrupting network users, services or equipment;
 - g) Private purposes such as marketing or business transactions;
 - h) Solicitation for religious or political causes;
 - i) Not-for-profit business activities inconsistent with the County's mission or unrelated to County business;
 - j) Private advertising of products or services;
 - k) For any activity meant to foster personal gain.
21. When sending confidential information, ~~all files must be encrypted and a password sent in a separate e-mail~~ the email message and any attachments must be encrypted using the county's encryption service. This applies even when sending a file through a secure network (e.g., HIN,

3

Adopted ~~6/24/2010~~ Resolution ~~192-10~~ Last revised

HSEN, etc.).

Adopted ~~6/24/2010~~ Resolution ~~192-10~~ Last revised

22. For a User to be able to receive emails on their County or Personal cell phones or devices the User must read “Cortland County’s Cellular Telephone/Telephone/Wireless Network Device Policy” and sign the “Personal Cellular Telephone and County eMail Agreement” along with their Department Head.

10. Acceptable and Unacceptable Use Policy

10.1 Acceptable Use

Users are responsible for exercising good judgment regarding the use of the County’s information resources. The County’s computers or networks shall not be used for personal or commercial use or to facilitate unethical or criminal activities. The County’s computers and networks are only to be used for official County business.

Communications by users from a County e-mail address must contain the following disclaimer:

This e-mail, including any attachments, may be confidential, privileged or otherwise legally protected. It is intended only for the addressee. If you receive this e-mail in error or from someone who was not authorized to send it to you, do not disseminate, copy or otherwise use this e-mail or its attachments. Please notify the sender immediately by reply e-mail and delete this e-mail from your system.

10.2 Unacceptable Use

Under no circumstances are users authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing County-owned resources.

Users found to be in violation of acceptable use policies may face disciplinary actions including employment termination as well as legal liability.

The listing below is by no means exhaustive, but attempts to provide a framework for activities that fall into the category of unacceptable use.

10.2.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions.

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by the County.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or movies, and the installation of any copyrighted software for which the County does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or national export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to anyone or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using a County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
7. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these actions are within the scope of regular duties. Examples:
 - a. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
 - b. Using any program/script/command or sending messages of any kind with the intent to interfere with or disable a user's terminal session via any means locally or via the Internet/intranet/extranet.
9. Port scanning or security scanning is expressly prohibited unless performed by authorized IT staff as required to perform regular job duties.
10. Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty (e.g., IT staff).
11. Circumventing user authentication or security of any host, network or account.
12. Providing information about or lists of County staff to parties outside County government, unless the information is considered public.
13. Using encryption on County information systems without providing the encryption keys to the IT Department according to specified procedures.
14. Intentionally changing hardware and software configurations as deployed by IT without written authorization from the County Administrator or the IT Department.

10.2.2 Email and Communications Activities

The following activities are strictly prohibited, with no exceptions.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) unless permission is granted by the County Administrator.
2. Any form of harassment via email, telephone or paging whether through language, frequency or size of messages.
3. Inappropriate cartoons or jokes or anything that may be construed as harassment or showing disrespect to others to include racial or ethnic slurs and gender- specific comments.
4. Unauthorized use or forging of email header information (a.k.a. e-mail spoofing).
5. Solicitation of e-mail for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
6. Creating or forwarding "chain letters," or other "pyramid" schemes of any type.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

10.2.3 Email Retention

Emails will remain on the County email archiver for Six (6) years at which time they will be removed permanently. If any emails are required to be kept for longer periods of time, for records retention or any other requirements, they should be copied to an appropriate place by the Person/Department that received the email prior to this time. In addition any documents that are "Scanned to email" will not be archived. If the documents that are scanned in need to be kept they need to be copied to an appropriate place by the Person/Department that scanned the document.

10.2.4 ~~Web Servers, MUDs, Network Games, Listservs, Other Computer Applications on~~ County Information Systems

Users may not ~~have web servers, Multi-User Dungeons (MUDs), network games,~~ unauthorized computer applications, file sharing programs or file transfer programs, ~~web servers (e.g., Napster, Gnutella, Kazaa, Morpheus, Audiogalaxy, BearShare, LimeWire, imesh, WiniN4X, Madster)~~ or listservs running on County information systems without written consent ~~from the SO and the IT Department Head.~~

10.2.5 Instant Messaging

Users are prohibited from using Instant Messaging (IM) on any County information resource, unless authorized in writing by the ~~SO user's department head and the IT Department Head.~~

10.2.6 Security Circumvention

Users must not attempt to compromise information system security measures in any way. Incidents involving unapproved system hacking or cracking, password, file decryption or similar attempts to compromise security measures will be considered violation of the County's information security policy. Unless specifically authorized by ~~the SO/IT~~ in consultation with the County Administrator, users, including IT staff, must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise the County's information systems security. Users, including IT staff, found in violation may face disciplinary measures, which may include immediate dismissal.

11. Privacy Expectations for Users

Users should be aware that Internet/intranet/extranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing and FTP are the property of the County and **thus users have no expectation of privacy.** The County reserves the right to access and monitor all messages and files on the County's network, PCs, laptops or workstations as deemed necessary and appropriate.

Backup copies of e-mail and data files are maintained and may be reviewed by authorized County personnel for legal, business or other reasons.

Authorized County personnel will perform monitoring. These authorized county personnel may monitor and log usage data, may review this data for evidence of violation of law or County policy, and may monitor all the activities and inspect the files and messages of specific users of County computers and networks. All communications including audio, video, text and images can be disclosed to law enforcement or third parties without prior consent of the sender or receiver.

11.1 Policy for Review and Release of Internal Data and Communications Files

This section defines who has access to internal data files and the authorization necessary to access those files. All requests are to be in writing or email from the appropriate person's County email account and sent to the ~~SO~~ Director of IT or his designee. The ~~County SO/IT Director~~ will make an initial determination as to the validity of the request. That decision is subject to review or appeal by the Chair of Legislature, appropriate Committee Chair or the County Attorney. At a minimum, the request should include the subject of the request, a reason, the type of data requested and a timeframe.

- Types of data and communications files, include but are not limited to:
 - Emails
 - Phone logs
 - Door access logs
 - Video

- Any data stored on county resources
- Access to the County's internal data files for:
 - Law Enforcement
 - Full access
 - Department Heads or their designees for their employees
 - Full access
 - Department Heads requesting information about an individual that is not their employee:
 - Get prior approval from the appropriate Department Head
 - If the department head declines then:
 - Get approval from the appropriate Legislative Committee chairman
 - A department head requesting information on another department head:
 - These requests will be handled by the Chair of the Legislature and the Chair of the Committee overseeing the subject of the request
 - Requests involving elected County officials:
 - These requests will be referred to the County Attorney
 - Any requests for data will be subject to standard County policies regarding privacy and confidentiality.

13. Security Tools

The ~~SO Director of IT~~ is authorized to acquire and employ the appropriate security tools necessary to ensure confidentiality, integrity and availability of the County's information system resources. Possession or use of security tools by other than specifically authorized IT staff is prohibited. Users found in violation may face disciplinary measures, which may include dismissal.

13.1 Information Technology Staff Permission to Use Security Tools

IT staff, who in their job duties will require the use of information security tools (a.k.a. hacking tools), must obtain permission from their immediate supervisor ~~and from the County SO~~ before such tools are acquired and used on the County's information resources.

14. Copyright and Licenses

Failure of users to observe copyright or license agreements may result in disciplinary action or legal action by the copyright owner and by the County. Users will be held personally liable for any violations of the copyright laws and license agreements. Supervisors will also be held personally liable if they knew about copyright and/or license violations and did not take any action to correct and to prevent copyright and licensing violations. Violations by users will be referred to the Personnel Office and the County Attorney for appropriate action.

16. Reporting Suspected Security Incidents / Violations

It is the user's responsibility to immediately report, in confidence, all suspected policy violations, suspected system intrusions or other conditions that might jeopardize the County's information security to their supervisor, Department Head, County Administrator, or ~~SO~~IT Director.

17. Violations

17.1 Non-Compliance

All users are required to comply with all the measures outlined in this policy. Violations of the provisions of this policy may lead to disciplinary action including termination and criminal prosecution.

17.2 Disciplinary Review

Violations will be dealt with according to current employee disciplinary practices.

17.3 Absence of Guidelines

The absence of specific guidance covering a particular situation does not relieve users from exercising the highest ethical standard applicable to the circumstances. When in doubt users should contact their immediate supervisor, the Department Head, or the [SOIT Director](#).

18. Cortland County Cyber Security Citizens' Notification Policy

18.1 Legal Requirement

Chapter 442 of the 2005 Session Laws require the County to adopt an information security breach and notification policy. This policy is consistent with the State Technology Law, section 208 as added by Chapters 442 and 491 of the laws of 2005.

18.2 Policy Content

This policy requires notification to impacted New York residents and non-residents. Cortland County values the protection of private information of individuals. Cortland County is required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and this policy.

19. The County's Information Systems Connections

19.1 External Connections

The IT Department must approve all external connections before any external connection is made and all connections must adhere to policies and procedures for security as set forth by the STG. All entities connected to the County network are required to maintain an up-to-date list of all external connections in use, and to provide the list to the IT Department. Non-compliance in maintaining such a list or not providing the list to IT allows it to terminate any connection to the County Network so as to preserve a secure environment. The [SOIT Director](#) is granted the authority to direct staff to remove connection points on the County's network under the [SOIT Director](#)'s control that pose a security risk to the County network.

The intent of this policy is to ensure that those responsible for the security of the County's network are aware of all external connections. Unless these connections are known, they cannot be secured. Any unsecured external connection can lead to security compromise of the entire County network.

19.2 Modems/Routers

The use of Modems/Routers on the Cortland County WAN or on any LAN connected to the WAN is not allowed. If there exists a business reason for a Modem/Router to be used, a business case will need to be presented to the STG. Only the IT Department ~~and the SO have~~ the authority to approve the use of a Modem/Router connection. The allowed Modem/Router connection shall be in accordance to the security policies and procedures set forth by IT for such connections.

This policy eliminates security vulnerabilities created by dial-up connections using modems. Modems are considered a weak link in security. For example, users may install a modem on their computers so they can access the Internet through their personal Internet Service Provider and, at

the same time, they are connected to a County LAN, and thus they are accessing the Internet in a manner that bypasses all County perimeter security—allowing a direct connection to the Internet.

19.3 Remote Access to the County's Network by Users

Remote access to the County WAN by the users shall only be via methods that ensure the security of the County's network and are approved by the STG. Only the ~~County Administrator or the SO~~IT Director ~~has~~es the authority to grant users remote access to the County's network, and only after reviewing with the department head the need for such access and access requirements.

~~19.4~~19.4 Wireless

~~Wireless access points/base stations connected to County networks must be approved and registered by the IT Department. "Peer-to-peer" wireless connections are not permitted.~~

~~Connecting County-owned equipment to non-County wireless access points without prior approval by the IT Department is prohibited.~~

~~19.5~~19.4 Air Cards

Air cards are not allowed unless authorized by the ~~user's d~~Department H~~ead~~, IT Director and the STG.

~~19.6~~19.5 Home Personal Computers/Devices

Home personal computers/~~D~~evices are considered non-secure devices. County data is not to be stored on an employee's home personal computer/Device.

If a home personal computer uses a Virtual Private Network (VPN) to access County data, then: 1) employee must receive approval from their Department Head and IT Department to use the VPN to access County data; and 2) employee is responsible for demonstrating that a home personal computer/~~D~~evice complies with all the requirements set forth in this document.

Accessing PHI using a home personal computer/~~D~~evice is not allowed.

~~19.7~~19.6 Third Party Access

Before any third party is allowed to connect to the County WAN, a third party connection agreement must be executed between the County and the third party. The ~~SO~~IT Director is the final approval authority for such agreements. The agreement will outline the third party's responsibilities and will hold them liable if they are not compliant with the agreement.

~~19.8~~19.7 Intermunicipality Agreements

Before any municipality is allowed to connect to the County WAN, an intermunicipality agreement must be executed between the county and the municipality. At a minimum the agreement outlines the roles and responsibility of the County and the municipality, and the agreement of the municipality to adhere to the security policies and procedures for connecting to the County WAN. The County Administrator ~~and the SO are is~~ the final approval authority of such agreements.

20. System Privileges/Access

20.9 Screen Savers

Users are required to have password protected screen savers activated. After 15 minutes of no activity, the screen saver blanks the screen. The user will need to re-authenticate to resume work.

20.10 Protecting Sensitive Information

If the information access by the user on a computer is classified as HIPAA related or is highly confidential, users must not leave their workstation without first logging-off or enabling a screen saver requiring re-authentication to continue work.

21. Log-In / Log-off Process

21.1 Network Log-in Banner Required

Every County system, where technically feasible, must employ a log-in banner that includes a warning notice. This notice must state: (1) the system is to be used only by authorized County users, and (2) by continuing to use the system, the user acknowledges that he/she is an authorized user and (3) consents to monitoring.

The use of a log-in banner is required to warn a potential user that only authorized users are allowed access, and they are responsible for their use of the County's information systems. In addition, users are put on notice that their actions may be monitored and consent to the monitoring.

21.2

User Authentication Required

At a minimum, positive identification for login into County information systems involves both a user-ID and a password, both of which are unique to an individual user. Other additional methods of authentication (e.g., token-based, smartcard, biometric) are to be considered where appropriate.

Formatted: Font: Bold

Formatted: Body Text, Right: 0.1", Space B
0.05 pt

21.3 Log-in Prompts

The login process for the County's information systems and applications must simply ask the user to log-in providing prompts as needed. Specific information about the County, the computer operating system, or the network configuration must not be provided until a user has successfully been authenticated.

If any part of the login sequence is incorrect, the person logging in must not be given specific feedback indicating the source of the problem - whether it was due to an invalid user-ID or to an invalid password. Instead, the person logging in must simply be informed that the login process -was incorrect.

22. Password Policy

22.4 Accountability

Users are accountable for all usage of their County provided accounts, and therefore shall not grant access to their account to any person or entity. The assumption by the County is that only the authorized user of an account has access to it. Therefore, the authorized user is accountable for all actions associated with the account. This maintains the audit ability of user actions, so the users cannot claim that someone else used their account to take unauthorized actions.

22.5 Password Disclosure

Users must never disclose their password(s) to anyone (including a superior) or to any entity under any circumstances.

If access to certain County resources is required for business purposes, the department head should approve the access. Under no circumstances should any user provide access to said resources via sharing a password or through other means. If a password is unintentionally disclosed or suspected

11

Adopted ~~6/24/2010~~ Resolution ~~192-10~~ Last revised

of being compromised, the user shall immediately change the password.

Adopted ~~6/24/2010~~ Resolution ~~192-10~~ Last revised

22.6 Positive Identification to Reset Password

To obtain a new or changed password, the system administrator must positively authenticate the identity of the person making the request. Only upon positively identifying the person will the system administrator issue a new password.

22.7 Password Selection

The first line of defense to prevent an attack against the County's information systems is the use of passwords that meet certain complexity requirements. Users are to choose a password that meets the following minimum complexity requirements:

- Must be at least 8 characters in length
- Include all of the following: Uppercase letters, lowercase letters and numbers
- May not include any part of your name in the password

22.8 Password Aging

All users will be automatically required to change their passwords periodically -- at least once every ninety (90) days or less.

22.9 Tracking Previous Passwords Used

If system software permits, a history file of passwords must be employed to prevent users from reusing passwords. The history file must minimally contain the last thirteen (13) passwords for each user-ID.

22.10 Password Storage

For all County information systems, passwords must be encrypted when stored or transmitted. Passwords must not be stored in unencrypted form in batch files, automatic login scripts, software macros, terminal function keys, computers without access control systems, or in other locations where unauthorized users might discover them. Similarly, passwords must not be written or produced in hard copy form and left in a place (e.g., a post-it note under the keyboard or next to the monitor screen) where unauthorized users might discover them.

22.11 Limited Number of Log-in Attempts

Access to an account will be locked-out if an unreasonable number of unsuccessful login attempts occur during a preset time period. The number of allowable failed login attempts and the length of the lockout is dependent on the criticality of the system and the sensitivity of the information.

25. Malicious Code

25.4 Malicious Code Eradication

Users are prohibited from attempting to eradicate malicious code from a system on the County's information system unless they do so in conjunction with authorized IT staff. If a virus or other malicious code is detected, IT is to be notified immediately. The computer is not to be shut down unless IT cannot be contacted.

26. Portable Devices (applies to laptop computers, handheld computers, PDAs which contain PHI (Protected Health Information), cell phones, and portable storage devices such as memory sticks, CDs, diskettes, MP3 players, digital pens etc.)

Portable devices are subject to safeguards to protect the confidentiality of the data. The guidelines below outline the steps needed to ensure the proper use and administration of portable devices.

1. All portable devices must be registered with IT. This includes all personally owned and County owned devices.
2. Any portable device should be used only by the individual that has registered it. Any portable device should not be used by any other individual outside the County government.
3. Access to data on portable devices and media must be protected by the use of authentication such as a password.
4. Any portable device or media should protect the data with a method of data encryption. Exceptions may be made by the Security Officer in conjunction with the STG. A record of the exceptions will be kept on the Portable Device Inventory.
5. Wireless data transmission to and from the portable device, including the syncing of PDAs, must be done via an encrypted connection.
6. Portable devices should be safeguarded from theft or loss the same way as a personal credit card.
7. All portable devices will indicate method of return to IT Department if found. Any misplaced portable device must be immediately reported to the department administrating them.
8. All portable devices are subject to the same security guidelines as workstation units including restricting visibility of display in public areas.
9. All data contained on portable devices must be backed up on a regular basis according to the policies and procedures set forth by IT.
10. Portable media that leaves the County worksite must follow all portable device requirements.
11. Portable devices are to be synchronized only to a County-approved computer.
12. Disposal of any portable device must follow the guidelines in this policy.
13. Sensitive information stored on a laptop computer shall be in encrypted form using the processes defined by the IT Department and approved by the SO.

26.1 Cloud/Online Storage

The use of cloud/online storage (Google Drive, Dropbox, etc.) is discouraged and will be considered on a case by case basis and subject to approval by the SO.

27. Encryption

27.1 Use of Encryption

Use of encryption on the County's information system will only be done using processes approved by the SO, and only for official County business. Users are forbidden to use encryption for any other purposes except for official County business.

27.2 Transmittal of Sensitive Information

Sensitive information that is to be transmitted on the County's WAN or via the Internet shall be encrypted. The requirement for encryption is set by the applicable department head. The IT Department sets and the SO approves the encryption processes to be used by the County to meet this requirement.

27.3 Storage of Sensitive Information

Sensitive information stored on County information systems must be encrypted. In addition, any archived (back-up copies) sensitive information also needs to be encrypted.

Encrypting stored sensitive information adds another security layer to the defense in depth concept. Encryption archived information prevents someone with access to the back-up tapes to access sensitive information.

27.4 Encryption Keys

14

Adopted ~~6/24/2010~~ Resolution ~~192-10~~ Last revised

Encryption keys used by the County shall be treated as confidential information. Access to encryption keys shall be strictly limited to those who have a need-to-know basis.

27.4.1 Encryption Key Escrow

Copies of all encryption keys will be kept in escrow and accessible by the County Administrator and the IT Department.

28. Transfer of Computer Equipment and Media

28.1 Internal to the County

The County strives strongly to protect the confidentiality of information entrusted to it. As the County upgrades computing equipment, equipment may be moved to other areas within the County. To protect information entrusted to the County, the proper measures need to be employed to ensure that all data is removed from the computer's storage media before the computer is relocated to another location within the County. The removal of such data shall be conducted by IT using methods approved by the SO that ensure that any previously stored information will not be recoverable.

28.2 Outside the County

As the County upgrades its computer systems, the County may decide to dispose of its old computers. Before any computer leaves County premises, IT shall be contacted and will ensure that all data stored on the computer is removed using methods approved by the SO ensuring that any previously stored information on the media is not recoverable.

29. Hardware and Software Configuration

Configurations and set-up parameters, as defined by the IT Department for deployed hardware and software must comply with County security policies and procedures. The configurations and parameters have been designed with security in mind as well as the County's ability to conduct business. Any changes in the configurations and set-up parameters of deployed hardware and software can undermine overall security, and thus are **forbidden**, unless approved in advance by the SO Director of IT or his designee. IT reserves the right to disconnect from the County network any hardware or software application with configuration or parameters that are not compliant.

Appendix B: Glossary

Authentication: The process to establish and prove the validity of a claimed identity.

Availability: This is the 'property' of being operational, accessible, functional and usable upon demand by an authorized entity, e.g., a system or a user.

~~Breach of~~ Breach – security of security: unauthorized acquisition of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the County.

Classification: The designation given to information or a document from a defined category on the basis of its sensitivity.

Cloud Storage: *(Also referred to as online storage)* A backup and storage service on the Internet. Cloud storage providers generally let users upload any size and type of computer file, whereas e- mail attachments often have limitations. Also called "online storage" and "public cloud storage," a customer's files are downloaded to anyone's computer with a Web browser and password. Many providers are freemium based, offering limited free storage and higher capacities for monthly fees. Others charge per-gigabyte-per-month.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Consumer reporting agency: an agency that assembles or evaluates consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties. A list of such agencies is compiled by the state attorney general and will be furnished to the County upon request.

Controls: Measures employed to satisfy the requirements set forth in this policy.

County Entity: County Entity, for the purposes of this policy, shall include all ~~County departments~~ County departments, offices, etc. over which the County Administrator has executive power.

Custodian: An employee or organizational unit acting as a caretaker of an automated file or database on behalf of a department.

Data: Data shall be defined as any information created, stored (in temporary or permanent form), produced or reproduced, regardless of the form of media. Data, in both electronic or hard copy form, may include, but is not limited to, personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Disaster: A condition in which information is unavailable, as a result of a natural or man-made occurrence that is of sufficient duration to cause significant disruption in the accomplishment of the County's business objectives as determined by the County leaders.

Disruption: Activities such as network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

16

Adopted ~~6/24/2010~~ Resolution ~~192-10~~ Last revised

Encryption: Rendering data unintelligible to anyone without a password.

Adopted ~~6/24/2010~~ Resolution ~~192-10~~ Last revised

ePHI: (electronic protected health information) Information that is defined as “protected health information” under HIPAA.

Firewall: A Security device that creates a barrier between an internal network and an external network.

FOIL: Freedom Of Information Law

Handheld Computer: Small computer running portable version of operating system.

HIPAA: The Health Insurance Portability and Accountability Act of 1996. This act affects the confidentiality and security practices of several departments within the County including Department of Social Services, Mental Health Department, and the Health Department.

Incident: Considered to be any adverse event that threatens the confidentiality, integrity or accessibility of information resources.

Incident Response: The manual and automated procedures used to respond to reported network intrusions (real or suspected), network failures and errors, and other undesirable events.

Information: Information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

Information Assets: (1) All categories of automated information, including but not limited to: records, files, and databases, and (2) information technology facilities, hardware and software owned or leased by the County.

Information Security: The concepts, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure or inability to process the information -- be it temporary or permanent.

Instant Messaging (IM): The ability to exchange short messages online with co-workers or others. IM solutions can take several forms.

Integrity: The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

Internet: A system of linked computer networks, international in scope, that facilitates data transmission and exchange, which uses the standard Internet protocol, TCP/IP, to communicate and share data.

Intranet: The intranet is an internal (i.e., non-public) network that uses the same technology and protocols as the Internet.

Intrusion Detection: The monitoring of network activities, primarily through automated measures, to detect, log and report actual or suspected unauthorized access and events for investigation and resolution.

IT: Information Technology. (Usually refers to the IT Department.)

LAN: Local Area Network

Laptop Computer: Portable computer running standard operating system.

Malicious Code: Programming or files that are developed for the purpose of doing harm and exploiting data security, examples of which are viruses, worms, Trojan horses, spyware, and phishing.

Off-site Backup: Mechanism to backup or archive PHI in a physical location other than that in which the data is primarily stored.

Owner: The department responsible for maintaining the integrity of the data.

PDA: Personal Digital Assistant. Handheld device used to store a variety of personal information such as contacts and schedule. Capable of storing digital data such as PHI.

PHI: Protected Health Information. A HIPAA term for any information (such as name, address, photo, diagnosis, etc.) used in a health-related context that should be kept confidential.

Portable Media: Floppy Disk, CDROM, DVD, USB Hard Drive or other media designed to store data.

Portable Storage Device: Device used for storing data such as USB flash drives.

Procedures: Specific operational steps that individuals must take to achieve goals stated in policy.

Private information: Personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- (1) social security number;
- (2) driver's license number or non-driver identification card number; or
- (3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome.

Risk Assessment: The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.

Risk Management: The process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

Sensitivity: The potentially harmful impact resulting from disclosure, modification, or destruction of information.

SO: Security Official—appointed by the County Administrator; see job description.

STG: Security Task Group. At a minimum, this group is composed of the SO, a representative from IT and departments that are considered “covered entities” under HIPAA—Department of Social Services, Mental Health Department, and Health Department. See responsibilities listed within the Security Official Job Description, Appendix A.

System: An interconnected set of information resources under the same direct management control that shares common functionality. A system may include hardware, software, information, data, applications, or communications infrastructure.

Threat: A threat is a force, organization, or person which seeks to gain access to, or compromise, information. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat, its capability and resources, one can assess it and determine the likelihood of occurrence, as in risk assessment.

Trojan Horse: Is a program in which malicious or harmful code is contained inside an apparently harmless program and, when executed, performs some unauthorized and undesirable activity or function.

User: Any County entity, political subdivision, its employees, third party contractor(s) or business associate(s), or any other individual(s) authorized by such entities to access a system for legitimate government purpose.

Virtual Private Network (VPN): Is a way to use a public infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization’s network.

Virus: A malicious program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. Once in the new host, a virus may corrupt files, display unwanted messages, crash the host, etc.

Vulnerability: A weakness of a system or facility holding information which can be exploited to gain access to violate system integrity. Vulnerability can be assessed in terms by which the attack would be successful.

WAN: Wide Area Network—a network that connects two or more LANS.

Worm: A worm is a self-replicating piece of malicious software, similar to a virus, but requires no user action to activate it. A worm exploits weaknesses in operating systems and other applications to propagate itself to other systems.

Revisions

2/20/2015

Add definition of cloud/online storage and rules governing their use

2/25/2016

Added paragraph 6.11 New York State FOIL Request Law

8/11/2017

Added paragraph 11.1 Policy for Review and Release of Internal Data and Communications Files

11/16/2017

Added paragraph 7.22 Referring Users to the “Cortland County’s Cellular Telephone/Telephone/Wireless Network Device Policy” on receiving County email on their Cell phones or devices.

4/2/2018

Added to paragraph 10.2.3 stating that Documents scanned to email will not be saved on the email archiver.

1/5/2023

Review and update.

ON MOTION OF PAUL HEIDER, COMMITTEE CHAIR**AGENDA ITEM NO. 1****Authorize Agreement with Bell & Spina Architects for Specs for Cortland County Courthouse
Dome/Cupola Rehabilitation - Buildings and Grounds Department**

WHEREAS, the County was awarded a grant from the Dormitory Authority of the State of New York (DASNY) in the amount of \$2,396,000 for the restoration and preservation of the Cortland County Courthouse, AND

WHEREAS, the projects to be completed with this funding are the main entryway and the dome/cupola of the Cortland County Courthouse, AND

WHEREAS, to proceed with the dome/cupola project, there is a need to have engineering specifications drawn up, AND

WHEREAS, Bell & Spina Architects of 215 Wyoming Street Syracuse, NY 13204, has the expertise to draw up specifications for said projects, AND

WHEREAS, Resolution No. 70-22 authorized the allocation of \$1,000,000 of American Rescue Plan funding for the planning, preparation and implementation of repairs to the Cortland County Courthouse and the funding is available in Account No. A16205.52320.ARP, NOW THEREFORE BE IT

RESOLVED, that the County Administrator, upon approval of the County Attorney, or their designee, is hereby authorized and directed to execute a contract, for an amount not to exceed \$200,000, with Bell & Spina Architects, 215 Wyoming Street Syracuse, NY 13204, for the completion of the specifications for said project, AND BE IT FURTHER

RESOLVED, that the County Administrator, upon review and approval by the County Attorney or designee and subject to appropriation of funding, be and hereby is authorized to enter into an agreement with Bell & Spina Architects of 215 Wyoming Street Syracuse, NY 13204, for said purposes at a cost not to exceed \$200,000 to be paid from Account No. A16205.52320.ARP.

ON MOTION OF

RESOLUTION NO.

Approve Use of County Property for 2023 Pumpkinfest



Greatcortlandpumpkinfest@gmail.com

March 31, 2023

Cortland County Legislature
Buildings and Grounds Committee
Cortland County Office Building
60 Central Avenue
Cortland, New York 13045

Committee Chair Heider and Buildings and Grounds Committee Members:

Please find below several items for the consideration of the committee as they relate to the 2023 Great Cortland Pumpkinfest, being planned for October 7 and 8, 2023:

Item # 1

The Great Cortland Pumpkinfest Planning Committee requests the use of the County's portion of Courthouse Park for use October 6-9, 2023 for set up, the festival and tear down. It is also requested to allow for open container in the County's portion of Courthouse Park during the operating hours of the festival.

Item # 2

The Great Cortland Pumpkinfest Planning Committee requests the consideration of a proposal to use a portion of the County Office Building parking lot and the County's overflow lot to set up and operate the midway as part of the 2023 festival. Please see Attachment 1.

Item # 3

The Great Cortland Pumpkinfest Planning Committee requests the use of the County Office Building parking lot overnight between October 5 and October 6 for parking food trucks between days of the festival, if needed.

Thank you for your consideration of these items as we look to plan the 2023 Great Cortland Pumpkinfest. The Great Cortland Pumpkinfest provides all necessary event insurance in relation to this these requests. Should any questions arise, please don't hesitate to reach out.

Sincerely,

The Great Cortland Pumpkinfest Committee



Greatcortlandpumpkinfest@gmail.com

ATTACHMENT 1

The proposed site for the midway during the 2023 Great Cortland Pumpkinfest (October 7 & 8, 2023) is a portion of the County Office Building parking lot (see below pictures).

Main Event Amusements would bring rides and a generator for the festival, which would be on the asphalt. The company would also bring food booths which we propose to set up on the asphalt and the grass in front of the County Office Building. The grass area would also be used as additional vendor/non-profit booth space if approved.

Main Event Amusements would need to use the proposed space starting at 5 PM Thursday, October 5, 2023 for setup and inspection of rides. Main Event Amusements would also need the use of the County's overflow lot all day on Thursday, October 5, 2023 for unloading and staging. Set up would occur on Thursday (October 5, 2023) evening through Friday (October 6, 2023) with NYS inspection to occur after completion. The rides would be present for the duration of Pumpkinfest weekend.





01010111 01100101 00100111
 01110010 01100101 00100000
 01101000 01100101 01110010
 01100101 00100000 01110100
 01101111 00100000 01101000
 01100101 01101100 01110000
 00100001

**Information
Technology**

CORTLAND COUNTY

**Jack Hess
Director**

**Tom McGrath
Deputy Director**

March 27, 2023

Information Technology March 2023 Monthly Report

Executive Summary

- IT
 - Continue deployment of CrowdStrike end point protection services
 - The migration proceeding on schedule and should be complete by the end of April.
 - Printer/copier upgrade
 - IT will be contracting for an upgraded Toshiba high capacity/high volume printer.
 - The county's information security policy has been included for your review.
 - County wide paging and door lockdown
 - Both systems were tested and some deficiencies are in the process of being corrected.
 - Evaluate the door security
 - Reviewed door security with Buildings and Grounds Supervisor Chuck Miller.
- Highway
 - Purchased cameras for Recycling and Landfill
 - Landfill cameras have been delivered and waiting on our vendor to finish cabling.
 - Recycling cameras are in place and operating.
- DERC
 - Syracuse Utilities has been contacted and will be evaluating the condition of the conduit and whether or not it can be used. If it is viable, they will then thread the route to allow for a fiber pull when desired.
 - Release an RFP for IT equipment for the new dispatch center at 22 W. Court St.
- City of Cortland
 - Discuss shared IT services with the Mayor.

Attachment: IT 2023_03_Monthly_Report (11386 : IT Monthly Report)

Departmental Priorities and Focus

Create a clear vision of IT for the future

- Status: In Process
 - The next committee meeting April 19, 2023.
 - Topics for discussion
 - Multi-factor authentication
 - Revising the county's security policy
 - Business continuity/disaster recovery
 - Data retention
 - Proposed members
 - Jack Hess, IT – Chair
 - Tom McGrath, IT
 - Lisa Perfetti, Health – Security Officer
 - Beau Harbin, Legislature
 - Rob Corpora, County Administration
 - Savannah Hempstead, Legislature
 - Brooke Kemak, County Clerk
 - Andrea Herzog, Finance
 - James Harvey, DSS
 - Sharon MacDougall, Mental Health
 - Alicia Wheaton, Probation
 - John Gallagher, Sheriff
 - Scott Roman, DERC

Cyber Security

- Status: In Process
 - Work with the state to conduct a cyber event tabletop exercise

Disaster recovery and business continuity planning

- Status: In Process
 - This will be discussed in the IT Steering Committee meeting.

County Wide Services

- Provide mail and print services to all County departments
- Provide fast reliable computer network for entire County
- Prepare new computers for Departments
- Maintain and enhance application programs for various departments to provide accurate and timely reports
- Monitor our security posture to mitigate the threat of ransomware and other attacks
- Provide desktop support
- Telecommunications support
- Access control to County buildings
- Camera and security systems
- Respond to requests for email archiver information (FOIL requests, etc.)
- Respond to alerts from intrusion detection system (IDS)
- Assign Munis roles and permissions

Departments

- Aging
- Assigned Counsel
- Buildings and Grounds
- CAC
- CWCC
- County Administration
- County Attorney
- County Clerk
- DERC
- DMV
- DSS
- District Attorney
- Elections
- Finance
- Grant Administration
- Health
- Highway
- Legislators
- Mental Health
- Personnel
- Planning
- Probation
- Public Defender
- RPTS
- Recycling
- Sheriff
- Soil and Water Conservation District
- Solid Waste
- Treasurer
- Veterans

External Agencies

- SUNY Cortland
- Homer PD
- Homer FD
- Cortland PD
- Cortland FD
- NYSP
- MAVAC
- Town of Cortlandville
- Town of Freetown

Contracts (Company, Service, Amount, Expires, Informational/Action Required)

• Radwin	Radio maint.	\$5,000/year	3/13/2023	Info.
• Trebron	Anti-Virus	\$7,110/year	5/25/2023	Info.
• Cisco	WebEx	\$10,000/year	6/30/2023	Info.
• GoDaddy	SSL Certificate	\$450/year	7/15/2023	Info.
• Barracuda	Email security gateway	\$5,000/year	8/23/2023	Info.
• Palo Alto	Firewall maint.	\$8,000/year	8/9/2023	Info.
• SHI	SAN maintenance	\$24,000/year	12/31/2023	Info.
• Barracuda	Email archiver maint.	\$5,688/year	2/26/2024	Info.
• Momentum	Phones – Service	\$10,991/year	3/31/2024	Info.
• Barracuda	Load balancer maint.	\$5,000/year	12/16/2024	Info.
• Nitel	Internet Service	\$12,000/year	12/31/2024	Info.
• Verizon	Internet Service	\$12,000/year	12/31/2024	Info.
• All Mode	Phones - Support	\$15,699/year	12/31/2024	Info.
• Westlaw	Online Legal Search	\$17,000/year	8/31/2026	Info.
• Toshiba Business Sol.	Copier/Printers	\$63,000/year	12/31/2023	Info.
• Pitney Bowes	Postage Meter	\$5,820/year	6/30/2027	Info.



CORTLAND COUNTY BUILDINGS & GROUNDS
Safety Office and Code Enforcement
60 Central Ave. B-28
Cortland, NY 13045-2746



5.2.a

Chuck Miller, B&G Superintendent 607-753-5068

David Clay Jr., BM Foreperson 607-753-5190

TO: B&G Committee

FROM: Chuck Miller, Superintendent, Safety and Code Enforcement Officer

DATE: 4/7/2023

SUBJECT: Activities Report for March 2023

Here are our monthly updates, please feel free to contact me if there are any questions or concerns or more information needed and I will accommodate in any way I am able.

We had 0 days of full staff due to time off and medical as well as open positions, we are currently short 2 custodians and 1 maintenance mechanic due to health issues and vacancies,

- 1) I have investigated incidents for the Safety office, and recorded over 15+ reports.
- 2) Completed Federal injury report census
- 3) KONE contract for Court House elevator is nearly completed, should be back by this meeting, expected start July-August 2023 3-4-week completion.
- 4) All contracts are in process for Court House step project, 1 completed 2 pending. Kick off meeting to took place April 3rd, more to come with this.
- 5) Bell and Spina to meet with Ms. McDougal on final floor plans and space occupation.
- 6) Bid process for Court House/City Court completed, award Bell and Spina Contract is complete and planning has begun.
- 7) Staffing issues continue interviewing week of April 3rd for final custodial position.
- 8) Met with State Courts and reviewed plan for alternate entrance during step construction.
- 9) Attended meetings on Court House, Personnel, Crescent Commons, Budget, PERMA, and One Group, Court House Committees and work groups, Bell and Spina, Violence in the work place, safety.
- 10) Worked with Mr. Hess from IT to address any entrance and safety issues that we may have.
- 11) Receiving proposals for Boiler water testing and Legionella testing for State requirements.
- 12) Renovations in Probation office complete. Moves of that department began April 3rd, project to have Probation moved completely in April, then begin County Clerk move at completion of elevator renovation.
- 13) Snow removal continues.
- 14) Addressing gym scheduling issues with Cortland Youth Bureau with Civil Service exams
- 15) Equipment for Age Well Center has begun to arrive and installations are already in progress.
- 16) Completed Code and Safety reporting to New York State
- 17) Working with Bell and Spina on area entryways and dome renovations to prepare specs and bid documents
- 18) Elevator project going well at County Office Building expect it to be operational soon if not by this meeting.
- 19) Working on repairs and upgrade to fire alarm system at County Office Building
- 20) Repairing flooring at Dwyer Park that was damaged by moisture from old cooler door
- 21) Working with new contract with Petcosky on sprinkler repairs and upgrades at Dwyer Park as well as Recycling, and annual testing and certification.

This fiscal season we have a number of small and large projects on the agenda, we will continue to work with all involved to keep everything running as smoothly as possible through this process. Please, if anyone has any questions, concerns, or issues, let's address them sooner than later. Communication will be key throughout this entire process.

Attachment: Departmental activities report March 2023.2 (11406 : Buildings & Grounds Activities and Time Line Reports)



CORTLAND COUNTY BUILDINGS & GROUNDS
Safety Office and Code Enforcement
60 Central Ave. B-28
Cortland, NY 13045-2746



5.2.a

Chuck Miller, B&G Superintendent 607-753-5068

David Clay Jr., BM Foreperson 607-753-5190

Respectfully
Chuck Miller
Superintendent of Building and Grounds
Code/Safety officer

Attachment: Departmental activities report March 2023.2 (11406 : Buildings & Grounds Activities and Time Line Reports)

Buildings and Grounds Timeline updates April 2023

Courthouse Stairs

Bids 27 Sept 2022, received and calculated, resolution passed 12/22/22
 Award December 2022
 Shop Drawings January 2023 Completed
 Kick off meeting was Monday
 Construction Mid-April to end of August 2023 (3-4 months)
 Beard Electric is to move fiber optic out from under the stairs into the building

111 Port Watson

Programing 30 Sept 2022 Not yet completed
 Schematic Design Base release was March of 2023
 Construction Doc Mid-May 2023
 Bidding End of May 2023
 Award June 2023
 Construction Duration August 2023 – August 2024 (10 – 12 Months)
 Meeting scheduled to discuss final floor plans and construction
 Historic eligibility being discussed and is delaying project a bit but they have submitted proposal to address SHPO concerns, 4/1/2023

2/20/2023

After Sharon's return, Mr. Spina had COVID, they continue programming.

City Court Relocation

Scope / Design Verification and design in process, RFQ changed to RFP, Courts request interview process for selection, released for Architect/Engineering Completed
 Award of Bid for Architectural February 2023 COMPLETE, Bell and Spina contract complete planning meeting is scheduled.
 Planning stages have begun. Meeting with 6th Judicial scheduled
 Construction Docs. April May 2023
 Bidding June 2023
 Award July 2023
 Construction Duration July-August start in 2023 (3 months) pending successful bid and on Contractor start date availability as well as elevator modernization schedule.

County Office Building Elevator renovation

Final walk through on January 18th, for set up
 Contract is signed back in County Attorney's office. September 2022
 Parts are ordered, expected to arrive Mid-January 2023 Delayed
 Tentative start date Mid-late February
 Once all parts are here installation expected to take 3 weeks, parts not all here will be pushed till after the first of the year so as to not interfere with the holidays and prolong process.
 Projected March 13th start date, Started on date
 Completion to be determined, expecting 2-3 weeks for completion
 Project going well to this point.
 Test runs scheduled for April, 5th and 6th, still going well

Buildings and Grounds Timeline updates April 2023

Court House Elevator renovation

Screening process OMNIA bid through KONE
 Initial walk through took place August 25th 2022
 Contract with KONE completed and returned
 Final cost \$265,000
 Lead time on equipment is approximately 4 months
 Start date for install should July-August 2023

3rd Floor HVAC project

Final engineering and checks complete
 One more walkthrough completed in January
 Equipment appears to be available for the most part
 Final cost of construction due, still not received
 pending project cost,
 Now adjusting construction goals and coverage, 2/27/23
 New plan being processed with less coverage. 3/20/2023

Court House entry areas and stone work

Contact made with Architect for cost to prepare Bid and Construction documents January 2023
 Timeline to be updated as information arrives
 Architects estimate arrived 2/27/2023 for Dome
 Architects estimates and proposal arrived
 Exterior Cleaning of stone added to the request 2/23
 Contract awarded to Bell and Spina for architectural and engineering of all proposed repairs.
 3/23

Court House Dome restoration

Contact Made with Architect for cost to prepare Bid and Construction documents January 2023
 Timeline to updated as information becomes available would be a 2024 Project