

October 22, 2014

The meeting was called to order by Chairman Norman L. Marsh.

The invocation was given by Rev. leFeber.

The Attendance Roll Call disclosed one Legislator absent - Murphy.

* * * * *

MR. BOSER moved, seconded by Mrs. Stockman that the minutes of the October 8, 2014 session be approved. Carried.

* * * * *

CHAIRMAN MARSH called up **Act No. 462-2014** and asked that it be read.

Approved by 7 members of the Finance Committee and 4 members of the Development and Agriculture Committee.

The following Legislator requested his name be listed as an additional sponsor: "Mr. Koch".

MRS. STOCKMAN moved, seconded by Mr. Teachman to amend Act No. 462-2014 as follows: In the first Resolved, add after "Program,": "which contribution shall be contingent upon receipt of the Community Services Block Grant by Cattaraugus Community Action, Inc.,". Carried.

Adopted, as amended, October 22, 2014 by voice vote. Ms. Edstrom was absent from floor for vote.

* * * * *

ACT NO. 475-2014 by Ms. Edstrom, Mrs. Stockman, Mr. Weller and Mr. Koch
and Mr. Padlo¹

**BID ACCEPTANCE FOR PURCHASE OF A 12 PASSENGER VAN
(Department of Social Services)**

Pursuant to Section 103 of the General Municipal Law and
Sections 215 of the County Law.

WHEREAS, the Clerk of the Legislature was authorized to advertise for sealed bids for the purchase of one (1) new and unused, 2014 or newer, 12 passenger van, according to specifications provided by the Public Works Committee, and

WHEREAS, the lowest responsible bid received meeting specifications was the bid of Emerling Chevrolet, Inc., 900 Boston State Road, Boston, New York 14025, for the purchase of one (1) new and unused, 2014 or newer, 12 passenger van, for an amount of \$26,217.00, and

WHEREAS, sufficient funds are included in the budget to cover the cost of the aforementioned van, now, therefore, be it

RESOLVED, that the bid of Emerling Chevrolet, Inc., be, and the same hereby is, accepted, for a term commencing upon Notice of Award and terminating 120 days thereafter, and be it further

RESOLVED, that the vouchers accordingly certified by the Commissioner of the Department of Public Works be audited by the Auditor and paid by the County Treasurer.

No State Bid.

Twenty sets of specifications were sent out.

Two bids were received meeting specifications.

Approved by 8 members of the Finance Committee, 9 members of the Public Works Committee and 6 members of the Human Services Committee.

¹The following Legislator requested his name be listed as an additional sponsor: "Mr. Padlo".

Adopted October 22, 2014 by voice vote.

ACT NO. 476-2014 by Mr. Weller and Mr. Koch

**AUTHORIZING THE CHAIR TO EXECUTE CONTRACT
WITH NATIONAL JOINT POWERS ALLIANCE
FOR COOPERATIVE PURCHASING PROGRAM**

Pursuant to Section 450 of the County Law.

WHEREAS, the National Joint Powers Alliance (NJPA) is a public agency that serves as a member-focused cooperative for over 50,000 member agencies and offers a multitude of cooperatively contracted products, equipment and service opportunities to educational and governmental entities, and

WHEREAS, the NYS Office of General Services (OGS) is a member of, and purchases through, the NJPA, and

WHEREAS, the Department of Public Works is desirous of becoming a member of the NJPA to purchase supplies, materials, equipment or services through the current and active competitive bidding process exercised by NJPA on behalf of governmental and other qualifying agencies, and

WHEREAS, there is no cost, obligation or minimum contract purchasing requirement to join or participate in the NJPA contract purchasing program, and

WHEREAS, it is necessary to execute a "Joint Exercise of Powers Agreement" in order to participate in the aforementioned purchasing cooperative, now, therefore, be it

RESOLVED, that the Chair of the Legislature be, and hereby is, authorized and directed to execute an agreement, on behalf of Cattaraugus County, with the National Joint Powers Alliance, in order to become a member of the above-described cooperative purchasing group, for a term commencing October 23, 2014 to continue in full force and effect until terminated by either party hereto, according to the above-described terms.

Approved by 8 members of the Finance Committee and 9 members of the Public Works Committee.

Adopted October 22, 2014 by voice vote.

ACT NO. 477-2014 by Mr. Snyder, Sr.

UPDATING AND RE-ESTABLISHING CATTARAUGUS COUNTY CAPITAL ASSET POLICY

Pursuant to GASB No. 34.

WHEREAS, Act 313-2001 established the Cattaraugus County Capital Asset Policy,
and

WHEREAS, it is necessary to update and re-establish the aforementioned policy,
now, therefore, be it

RESOLVED, that effective immediately, the following shall constitute the Capital Asset Policy for Cattaraugus County, provided, however, that the adoption of this resolution shall not negate or otherwise affect any actions taken prior to the effective date hereof pursuant to Act 313-2001:

**County of Cattaraugus
Capital Asset Guide**

1. Capital Asset Definitions and Guidelines
 - 1.1 Capital Asset Classification
 - 1.2 Capitalization Thresholds
 - 1.3 Capital Asset Acquisition Cost
 - 1.4 Capital Asset Donations
 - 1.5 Leased Equipment
 - 1.6 Depreciating Capital Assets
 - 1.7 Residual Value
 - 1.8 Sale of Capital Assets
 - 1.9 Computation of Gain and Loss from Sale of Assets
 - 1.10 Trade-in of Assets
 - 1.11 Assets Held in Trust
 - 1.12 Impairment of Capital Assets
 - 1.13 Departmental Inventories
 - 1.14 Capital Asset Manager/Departmental Custodian
2. Capital Asset Categories
 - 2.1 Land and Land Improvements
 - 2.1.1 Land Definition
 - 2.1.2 Land Improvement Definition
 - 2.1.3 Depreciation Methodology
 - 2.1.4 Capitalization Threshold

- 2.2 Buildings and Building Improvements
 - 2.2.1 Building Definition
 - 2.2.2 Building Improvement Definition
 - 2.2.3 Depreciation Methodology
 - 2.2.4 Capitalization Threshold
 - 2.2.5 Maintenance Expense
- 2.3 Facilities and Other Improvements
 - 2.3.1 Facilities Definition
 - 2.3.2 Other Improvements Definition
 - 2.3.3 Depreciation Methodology
 - 2.3.4 Capitalization Threshold
- 2.4 Infrastructure
 - 2.4.1 Infrastructure Definition
 - 2.4.2 Infrastructure Improvements
 - 2.4.3 Jointly Funded Infrastructure
 - 2.4.4 Modified Approach vs. Depreciation
 - 2.4.5 Maintenance Costs
 - 2.4.6 Preservation Costs
 - 2.4.7 Additions and Improvements
 - 2.4.8 Depreciation Methodology
 - 2.4.9 Capitalization Threshold
- 2.5 Machinery and Equipment
 - 2.5.1 Equipment Definition
 - 2.5.2 Jointly Funded Personal Property
 - 2.5.3 Depreciation Methodology
 - 2.5.4 Capitalization Threshold
- 2.6 Computers
 - 2.6.1 Computers Definition
 - 2.6.2 Depreciation Methodology
 - 2.6.3 Capitalization Threshold
- 2.7 Software
 - 2.7.1 Software Definition
 - 2.7.2 Depreciation Methodology
 - 2.7.3 Capitalization Threshold
- 2.8 Construction in Progress
 - 2.8.1 Construction in Progress Definition
 - 2.8.2 Depreciation Methodology
 - 2.8.3 Capitalization Threshold
- 2.9 Network Equipment
 - 2.9.1 Network Equipment Definition
 - 2.9.2 Depreciation Methodology
 - 2.9.3 Capitalization Threshold

1. CAPITAL ASSET DEFINITIONS AND GUIDELINES

Capital assets are real or personal property that have a value equal to or greater than the capitalization threshold for the particular classification of the asset and have an estimated life of greater than one year.

The County has invested in a broad range of capital assets that are used in the County's operations, which include:

- Land and land improvements
- Buildings and building improvements
- Facilities and other improvements
- Infrastructure
- Machinery and Equipment
 - Furniture and equipment
 - Vehicles, boats and aircraft
- Network Equipment
- Computers
- Software
- Intangible assets
- Construction in progress

1.1 Capital Asset Classification

1.1.1 Assets purchased, constructed or donated that meet or exceed the Treasurer's established capitalization thresholds or minimum reporting requirements must be uniformly classified.

1.1.2 Departments will follow the County Treasurer's accounting standards for establishing the historical cost for each asset.

1.2 Capitalization Thresholds

Standard capitalization thresholds for capitalizing assets have been established for each major class of assets. All County entities are required to use these thresholds.

Class of Asset	Threshold
Land/land improvements	\$ 5,000
Buildings/building improvements	\$50,000
Facilities & other improvements	\$50,000
Infrastructure	\$50,000
Machinery & Equipment	\$ 1,000*
Computers	Capitalize All
Software	Capitalize All
Construction in Progress	\$50,000
Leasehold improvements	\$100,000
Network Equipment	Capitalize All

1.3 Capital Asset Acquisition Cost

1.3.1 Capital assets should be recorded and reported at their historical costs, which includes the vendor's invoice (plus the value of any trade-in), plus sales

tax (if applicable), initial installation cost (excluding in-house labor), modifications, attachments, accessories or apparatus necessary to make the asset usable and render it into service. Historical cost also includes ancillary charges such as freight and transportation charges, site preparation costs, professional fees, and computer software user licenses (if licenses cover a period of more than one year).

- 1.3.2 Historical cost does **not** include user licenses that cover only one year, nor do they include training costs, extended warranty costs, and maintenance costs – these costs should be expensed.

The cost of capital assets for **governmental activities** does not include capitalized interest. However, interest is capitalized on:

- Assets that are constructed or otherwise produced for an enterprise's own use (including assets constructed or produced for the enterprise by others for which deposits or progress payments have been made)
- Assets intended for sale or lease that are constructed or otherwise produced as discrete projects (for example, real estate developments)

- 1.3.3 Assets that *do not* qualify for capitalization of interest include:

- Assets acquired for governmental activities (interest will be reported in the statement of activities as a separate line item)
- Assets that are in use or ready for their intended use in the earning activities of the enterprise
- Assets that are not being used in the earning activities of the enterprise and that are not undergoing the activities necessary to get them ready
- Assets acquired with gifts and grants that are restricted by the donor or grantor to acquisition of those assets to the extent that funds are available from such gifts and grants.

1.4 Capital Asset Donations

- 1.4.1 Donated capital assets should be reported at fair value at the time of acquisition plus ancillary charges, if any. Donations are defined as voluntary contributions of resources to a governmental entity by a non-governmental entity.

****Note:** *A voluntary contribution of resources between governmental entities is not a donation.*

Fair Value: The amount at which an asset could be exchanged in a current transaction between willing parties.

- 1.4.2 Modified Accrual Basis - Governments should not report revenue from the donation of a capital asset when using the modified accrual basis except in the following situation:

If an entity receives a donation of a capital asset and intends to sell the asset immediately, revenue should be recognized in the period the asset is donated, and the capital asset should be reported in the same fund used to report the

revenue as "Assets Held for Sale." Intent to sell should be evidenced by a sale of or contract to sell the capital asset before financial statements are issued.

Revenue should be measured at the amount at which the capital asset is sold or its contract price. If the entity does not intend to sell the donated capital asset immediately or does not meet the criteria for intent to sell stated above, the donation should not be reported in the operations of the governmental funds.

Revenue from donations of financial resources such as cash, securities or capital assets should be recognized when the entity has an enforceable legal claim to the donation and when it is probable the donation will be received - regardless of when the financial resources are actually received. Revenue should be measured at the fair value of financial resource donated.

- 1.4.3 Full Accrual Basis – According to GASB Statement No. 33, *Accounting and Financial Reporting for Non-Exchange Transactions* entities currently using proprietary fund accounting must recognize capital asset donations as revenues and not as contributed capital.

Governmental funds will have to meet the standards of GASB Statement No. 33. Donations must be recorded and reported as fair value on the date of acquisition based on a reasonable market study. Recipients of donated capital assets will recognize the donation and related revenue when the transaction is complete and the assets are received, providing all eligibility requirements have been met. Promises of capital asset donations should be recognized as receivables and revenues (net of estimated uncollectible amounts) when all applicable eligibility requirements have been met, providing that the promise is verifiable and the resources are measurable and probable of collection.

In some cases, donated capital assets are given with the stipulation (time requirement) that the assets cannot be sold, disbursed or consumed until a specified number of years have passed or a specific event has occurred. For such cases, the capital asset should be reported in the statement of Net Assets as "Net Assets-Restricted" as long as the restrictions or time requirements remain in effect.

1.5 Leased Equipment

- 1.5.1 Equipment should be capitalized if the lease agreement meets any one of the following criteria:
- The lease transfers ownership of the property to the lessee by the end of the lease term.
 - The lease contains a bargain purchase option.
 - The lease term is equal to 75 percent or more of the estimated economic life of the leased property.
 - The present value of the minimum lease payments at the inception of the lease, excluding executory costs, equals at least 90 percent of the fair value of the leased property.

- 1.5.2 Leases that do not meet any of the above requirements should be recorded as an operating lease and reported in the notes of the financial statements.

1.6 Depreciating Capital Assets

- 1.6.1 Capital assets should be depreciated over their estimated useful lives unless they are inexhaustible.

- 1.6.2 The straight-line depreciation method (historical cost less residual value, divided by useful life) will be used by all county entities. Depreciation data will be calculated and stored by the Treasurer's office for each eligible asset.

Accumulated depreciation will be summarized and posted to the accounting general ledger.

1.7 Residual Value

In order to calculate depreciation for an asset, the estimated residual value must be declared before depreciation can be calculated. Residual value is the amount for which an asset can be sold at the end of its useful life. The use of historical sales information becomes invaluable for determining the estimated residual value. Proceeds from sale of assets must be netted against residual value in computing net gain or loss from sale.

1.8 Sale of Capital Assets

- 1.8.1 When an asset is sold to a non-county entity or another county department, a gain or loss must be recognized in the annual report when:

- Cash is exchanged and the amount paid does not equal the net book value of the asset
- Cash is not exchanged and the asset is not fully depreciated or has a residual value

- 1.8.2 A gain or loss is not reported when:

- Cash exchanged equals the net book value and the asset does not have a residual value
- Cash is not exchanged and the asset is fully depreciated and has no residual value

1.9 Computation of Gain and Loss from Sale of Assets

- 1.9.1 To compute a gain or loss, proceeds received must be subtracted from the asset's net book value.

Example:	Asset's Historical Cost	\$10,000
	Less Accumulated Depreciation	\$ 7,000
	Net Book Value	\$ 3,000
	Subtract Proceeds Received	\$ 2,000
	Loss from Sale of Asset	\$ 1,000

- 1.9.2 If the asset has been fully depreciated and has a residual value, then the proceeds must be subtracted from the residual value to compute the gain or loss.

Example:	Asset's Historical Cost (residual value - \$1,000)	\$10,000
	Less Accumulated Depreciation	\$ 9,000
	Residual Value	\$ 1,000
	Subtract Proceeds Received	\$ 2,000
	Gain from Sale of Asset	\$ 1,000

1.10 Trade-in of Assets

1.10.1 When recording a trade-in of similar assets, agencies must use a book value basis for the assets surrendered or acquired.

- When assets are exchanged and no monetary consideration is paid or received, the cost of the asset acquired is recorded at the carrying (book) value of the asset surrendered.
- Where monetary consideration is given, the new asset must be recorded at the sum of the cash paid plus the book value of the asset surrendered.

1.10.2 Dissimilar assets - When recording a trade-in of dissimilar assets, agencies must:

- Record the value of the asset being traded and the resulting transaction for acquiring the new asset, using the fair value of the asset being traded.
- If cash is used to purchase the asset, agencies must record the transaction for the new asset as cash paid plus the fair value of the asset surrendered.

1.11 Assets Held in Trust

Capital assets held by an agency on behalf of a non-county entity (such as art collections owned by families, estates and others) and that are under the temporary control of the department should be recorded in an agency fund until returned to the owners. This includes assets owned by the federal government that have been loaned to a county entity. Assets held in trust must be reported to the Treasurer using the appropriate acquisition and disposal method for such assets.

1.12 Impairment of Capital Assets

This section establishes accounting reporting standards for impairment of capital assets. A capital asset is considered impaired when its service utility has declined significantly and unexpectedly. If evidence is available to demonstrate that the impairment will be temporary, the capital asset will not be written down. Impaired capital assets that are idle should be reported, regardless of whether the impairment is considered permanent or temporary. Capital assets that become impaired must be reported to the Treasurer's Office to identify the write down of the capital asset. Common indicators of impairment include:

- Evidence of physical damage, such as for a building damaged by fire or flood,

when the level of damage is such that restoration efforts are needed to restore service utility.

- Enactment or approval of laws or regulations or other changes in environmental factors, such as new water quality standards that a water treatment plant does not meet (and cannot be modified to meet).
- Technological development or evidence of obsolescence, such as that related to a major piece of diagnostic or research equipment (for example, a magnetic resonance imaging machine or a scanning electron microscope) that is rarely used because newer equipment provides better service.
- A change in the manner or expected duration of use of a capital asset, such as closure of a school prior to the end of its useful life.
- Construction stoppage, such as stoppage of construction of a building due to lack of funding.

1.13 Departmental Inventories

All assets not meeting the threshold of Capital Assets must be included in a departmental inventory for fixed or movable equipment and buildings. The department head or their designee(s) shall be required to maintain the department inventory and verify the inventory at least annually. All inventories must be maintained in an auditable format, which shall include item description, total purchase price, date of acquisition, model number, serial number, location of item, vendor, and expenditure account. All inventories are subject to unannounced internal and independent audits.

1.14 Capital Asset Manager/Departmental Custodian

1.14.1 The Cattaraugus County Legislature designates and authorizes the County Treasurer, or its designee, to act as Capital Asset Manager. It is the responsibility of the Capital Asset Manager to develop and maintain all detailed rules and regulations with respect to Capital Assets. The Capital Asset Manager shall be responsible for a physical inventory of all capital assets at least once every four years.

1.14.2 The Cattaraugus County Legislature designates and authorizes the department head of each department, or its designee, to act as Departmental Custodian. The Departmental Custodian shall file the appropriate records with the Capital Asset Manager and verify the departmental asset inventory at least annually.

2. **CAPITAL ASSET CATEGORIES**

2.1 Land and Land Improvements

2.1.1 Land Definition

Land is the surface or crust of the earth, which can be used to support structures, and may be used to grow crops, grass, shrubs, and trees. Land is characterized as having an unlimited life (indefinite).

2.1.2 Land Improvement Definition

Land improvements consist of betterments, site preparations and site improvements (other than buildings) that ready land for its intended use. The costs associated with improvements to land are added to the cost of the land.

2.1.3 Depreciation Methodology

Land and land improvements are inexhaustible assets and are not depreciated.

2.1.4 Capitalization Threshold

The capitalization threshold for land and land improvements is \$5,000.

2.1.5 Examples of Expenditures to be Capitalized as Land and Land Improvements:

- Purchase price for fair market value at time of gift
- Commissions
- Professional fees (title searches, architect, legal, engineering, appraisal, surveying, environmental assessments, etc.)
- Land excavation, fill, grading, drainage
- Demolition of existing buildings and improvements (less salvage)
- Removal, relocation, or reconstruction of property of others (railroad, telephone and power lines)
- Interest on mortgages accrued at date of purchase
- Accrued and unpaid taxes at date of purchase
- Other costs incurred in acquiring the land
- Water wells (includes initial cost for drilling, the pump and its casing)
- Right-of-way

2.2 Buildings and Building Improvements

2.2.1 Building Definition

A building is a structure that is permanently attached to the land, has a roof, is partially or completely enclosed by walls, and is not intended to be transportable or moveable. Buildings that are an ancillary part of the county's highway network, such as rest area facilities and toll buildings will be reported as infrastructure rather than as buildings.

2.2.2 Building Improvement Definition

Building improvements are capital events that materially extend the useful life of a building or increase the value of a building, or both. A building improvement should be capitalized as a betterment and recorded as an addition of value to the existing building if the expenditure for the improvement is at the capitalization threshold, or the expenditure increases the life or value of the building by 25 percent of the original life or cost. Subsequent improvements that change the use or function of the building shall be capitalized.

2.2.3 Depreciation Methodology

The straight-line depreciation method (historical cost less residual value divided by useful life) will be used for buildings, building improvements and their components.

2.2.4 Capitalization Threshold

The capitalization threshold for buildings and building improvements is \$50,000.

2.2.5 Examples of Expenditures to be Capitalized as Buildings:

Purchased Buildings

- Original purchase price
- Expenses for remodeling, reconditioning or altering a purchased building to make it ready to use for the purpose for which it was acquired
- Environmental compliance (i.e., asbestos abatement)
- Professional fees (legal, architect, inspections, title searches, etc.)
- Payment of unpaid or accrued taxes on the building to date of purchase
- Cancellation or buyout of existing leases
- Other costs required to place or render the asset into operation

Constructed Buildings

- Completed project costs
- Interest accrued during construction
- Cost of excavation on grading or filling of land for a specific building
- Expenses incurred for the preparation of plans, specifications, blueprints, etc.
- Cost of building permits
- Professional fees (architect, engineer, management fees for design and supervision, legal)
- Costs of temporary buildings used during construction
- Unanticipated costs such as rock blasting, piling, or relocation of the channel of an underground stream
- Permanently attached fixtures or machinery that cannot be removed without impairing the use of the building
- Additions to buildings (expansions, extensions, or enlargements)

Examples of Expenditures to be Capitalized as Improvements to Buildings

****Note:** For a replacement to be capitalized, it must be a part of a major repair or rehabilitation project, which increases the value, and/or useful life of the building. A replacement may also be capitalized if the new item/part is of significantly improved quality and higher value compared to the old item/part such as replacement of an old shingle roof with a new fireproof tile roof. Replacement or restoration to original utility level would not. Determinations must be made on a case by case basis.

- Conversion of attics, basements, etc., to usable office, clinic, research or classroom space
- Structures attached to the building such as covered patios, sunrooms, garages, carports, enclosed stairwells, etc.
- Installation or upgrade of heating and cooling systems, including ceiling fans and attic vents
- Original installation/upgrade of wall or ceiling covering such as carpeting, tiles, paneling, or parquet
- Structural changes such as reinforcement of floors or walls, installation or replacement of beams, rafters, joists, steel grids, or other interior framing

- Installation or upgrade of window or door frame, upgrading of windows or doors, built-in closet and cabinets
- Interior renovation associated with casings, baseboards, light fixtures, ceiling trim, etc.
- Exterior renovations such as installation or replacement of siding, roofing, masonry, etc.
- Installation or upgrade of phone or closed circuit television systems, networks, fiber optic cable, wiring required in the installation of equipment (that will remain in the building)
- Other costs associated with the above improvements

2.2.6 Maintenance Expense

The following are examples of expenditures not to capitalize as improvements to buildings. Instead, these items should be recorded as maintenance expense.

- Adding, removing and/or moving of walls relating to renovation projects that are not considered major rehabilitation projects and do not increase the value of the building
- Improvement projects of minimal or no added life expectancy and/or value to the building
- Plumbing or electrical repairs
- Cleaning, pest extermination, or other periodic maintenance
- Interior decoration, such as draperies, blinds, curtain rods, wallpaper
- Exterior decoration, such as detachable awnings, uncovered porches, decorative fences, etc.
- Maintenance-type interior renovation, such as repainting, touch-up plastering, replacement of carpet, tile, or panel sections; sink and fixture refinishing, etc.
- Maintenance-type exterior renovation such as repainting, replacement of deteriorated siding, roof, or masonry sections
- Replacement of a part or component of a building with a new part of the same type and performance capabilities, such as replacement of an old boiler with a new one of the same type and performance capabilities
- Any other maintenance-related expenditure which does not increase the value of the building

2.3 Facilities and Other Improvements

2.3.1 Facilities Definition

Assets (other than general use buildings) built, installed or established to enhance the quality or facilitate the use of land for a particular purpose.

2.3.2 Other Improvements Definition

Depreciable improvements made to a facility or to land that should be capitalized as a betterment if the improvement is at the capitalization threshold or the expenditure increases the life or value of the asset by 25 percent of the original cost or life period.

2.3.3 Depreciation Methodology

The straight-line depreciation method (historical cost less residual value divided by useful life) will be used for Facilities and Other Improvements.

2.3.4 Capitalization Threshold

The capitalization threshold for facilities and other improvements is \$50,000.

2.3.5 Examples of Expenditures to be Capitalized as Facilities and Other Improvements:

- Fencing and gates
- Landscaping
- Parking lots/driveways/parking barriers
- Outside sprinkler systems
- Recreation areas and athletic fields (including bleachers)
- Golf courses
- Paths and trails
- Septic systems
- Stadiums
- Swimming pools, tennis courts, basketball courts
- Fountains
- Plazas and pavilions
- Retaining walls

2.4 Infrastructure

2.4.1 Infrastructure Definition

Assets that are long-lived capital assets that normally are stationary in nature and can be preserved for a significantly greater number of years than most capital assets. Infrastructure assets are often linear and continuous in nature.

2.4.2 Infrastructure Improvements

Infrastructure improvements are capital events that materially extend the useful life or increase the value of the infrastructure, or both. Infrastructure improvements should be capitalized as a betterment and recorded as an addition of value to the infrastructure if the improvement or addition of value is at the capitalization threshold or increases the life or value of the asset by 25 percent of the original cost or useful life.

2.4.3 Jointly Funded Infrastructure

Infrastructure paid for jointly by the county and other governmental entities should be capitalized by the entity responsible for future maintenance.

2.4.4 Maintenance Costs

Maintenance costs allow an asset to continue to be used during its originally established useful life. Maintenance costs are expensed in the period incurred.

2.4.5 Preservation Costs

Preservation costs are generally considered to be those outlays that extend the useful life of an asset beyond its original estimated useful life, but do not increase the capacity or efficiency of the asset. Preservation costs should be

capitalized under the depreciation approach.

2.4.6 Additions and Improvements

Additions and improvements are those capital outlays that increase the capacity or efficiency of the asset. A change in capacity increases the level of service provided by an asset. For example, additional lanes can be added to a highway or the weight capacity of a bridge could be increased. A change in efficiency maintains the same service level but at a reduced cost. The cost of additions and improvements should be capitalized.

2.4.7 Depreciation Methodology

The straight-line depreciation method (historical cost less residual value, divided by useful life) will be used for infrastructure assets.

2.4.8 Capitalization Threshold

The capitalization threshold for infrastructure is \$50,000. Infrastructure already capitalized will remain capitalized.

2.4.9 Examples of Expenditures to be Capitalized as Infrastructure

- Highway and rest areas
- Roads, streets, curb, gutters, sidewalks, fire hydrants
- Bridges, railroads, trestles
- Canals, waterways, wharf, docks, sea walls, bulkheads, boardwalks
- Dam, drainage facility
- Radio or television transmitting tower
- Electric, water and gas (main lines and distribution lines, tunnels)
- Fiber optic and telephone distribution systems (between buildings)
- Light system (traffic, outdoor, street, etc.)
- Signage
- Airport runway/strip/taxiway/apron

2.5 Machinery and Equipment

2.5.1 Equipment Definition

Fixed or movable tangible assets to be used for operations, the benefits of which extend beyond one year from date of acquisition and rendered into service. Improvements or additions to existing personal property that constitute a capital outlay or increase the value or life of the asset by 25 percent of the original cost or life should be capitalized as a betterment and recorded as an addition of value to the existing asset.

Note: *Costs of extended warranties and/or maintenance agreements, which can be separately identified from the cost of the equipment, should not be capitalized.*

2.5.2 Jointly Funded Personal Property

Personal property paid for jointly by the county and other governmental entities should be capitalized by the entity responsible for future maintenance.

2.5.3 Depreciation Methodology

The straight-line depreciation method (historical cost less residual value divided by useful life) will be used for personal property.

2.5.4 Capitalization Threshold

The capitalization threshold for personal property is **\$1,000**. County departments who have a multiple year cost allocation plan or an indirect cost proposal **will not** be required to implement the new threshold until such time that they renegotiate their cost allocation plan or indirect cost proposal with their federal cognizant agency, such as the U.S. Department of Health and Human Services.

2.5.5 Examples of Expenditures to be Capitalized as Personal Property:

- Original contract or invoice price
- Freight charges
- Import duties
- Handling and storage charges
- In-transit insurance charges
- Sales, use, and other taxes imposed on the acquisition
- Installation charges
- Charges for testing and preparation for use
- Costs of reconditioning used items when purchased
- Parts and labor associated with the construction of equipment

2.6 Computers

2.6.1 Computers Definition

Technically, a computer is a programmable machine. This means it can execute a programmed list of instructions and respond to new instructions that it is given. Today, however, the term is most often used to refer to the desktop and laptop, and tablet computers that most people use. When referring to a desktop model, the term "computer" technically only refers to the computer itself – not the monitor. Some of the major parts of a personal computer (PC) include the motherboard, CPU, memory (or RAM), hard drive, video card, and any other internal devices/components.

2.6.2 Depreciation Methodology

The straight-line depreciation method (historical cost divided by the asset's useful life) will be used for computers.

2.6.3 Capitalization Threshold

All purchases of computers shall be capitalized, as there is no minimum dollar amount.

2.7 Software

2.7.1 Software Definition

- (i) Software is a generic term for organized collections of computer data and instructions, often broken into two major categories: system software that provides the basic non-task-specific functions of the computer, and application software which is used by users to accomplish specific tasks.

- (ii) System software is responsible for controlling, integrating, and managing the individual hardware components of a computer system so that other software and the users of the system see it as a functional unit without having to be concerned with the low-level details such as transferring data from memory to disk, or rendering text onto a display. Generally, system software consists of an operating system and some fundamental utilities such as disk formatters, file managers, display managers, text editors, user authentication (login) and management tools, and networking and device control software. System software is usually purchased with new computer purchases, as such will be included with the cost of the new computer.
- (iii) Application software, on the other hand, is used to accomplish specific tasks other than just running the computer system. Application software may consist of a single program, such as an image viewer; a small collection of programs (often called a software package) that work closely together to accomplish a task, such as a spreadsheet or text processing system; a larger collection (often called a software suite) of related but independent programs and packages that have a common user interface or shared data format, such as Microsoft Office, which consists of closely integrated word processor, spreadsheet, database, etc; or a software system, such as a database management system, which is a collection of fundamental programs that may provide some service to a variety of other independent applications.
- (iv) A *software license* comprises the permissions, rights and restrictions imposed on software (whether a component or a free-standing program). Use of software without a license could constitute infringement of the owner's exclusive right under copyright or, occasionally, patent law and allow the owner to sue the infringer.
- (v) Under a software license, the licensee is permitted to use the licensed software in compliance with the specific terms of the license. If there is a breach of the license, depending on the license, it may result in termination of the license and potentially the right of the owner to sue.
- (vi) A software vendor may offer a software license unilaterally (without giving the licensee the opportunity to negotiate for more favorable terms) such as in a shrink wrap contract, or even as part of a software license agreement with another party. Virtually all mass produced proprietary software is sold under some form or fashion of software license agreement. Custom software is often licensed under terms of which are specifically negotiated between the licensee and licensor.
- (vii) The total historical cost of software shall not include voluntary software maintenance fees.

- 2.7.2 Depreciation Methodology
The straight-line depreciation method (historical cost divided by the asset's useful life) will be used for software.
- 2.7.3 Capitalization Threshold
All purchases of software and software licenses valid for more than 1 year shall be capitalized, as there is no minimum dollar amount.
- 2.8 Construction in Progress
 - 2.8.1 Construction in Progress Definition
Construction in Progress reflects the economic construction activity status of buildings and other structures, infrastructure (highways, energy distribution systems, pipelines, etc.), additions, alterations, reconstruction, installation, and maintenance and repairs which are substantially incomplete.
 - 2.8.2 Depreciation Methodology
Depreciation is not applicable while assets are accounts for as Construction in Progress. See appropriate capital asset category when asset is capitalized.
 - 2.8.3 Capitalization Threshold
Construction in Progress assets should be capitalized to their appropriate capital asset categories upon the earlier occurrence of execution of substantial completion contract documents, occupancy, or when the asset is placed into service.
- 2.9 Network Equipment
 - 2.9.1 Network Equipment Definition
Network Equipment is made up of servers, switches and routers.
 - 2.9.2 Depreciation Methodology
The straight-line depreciation method (historical cost divided by the asset's useful life) will be used for software.
 - 2.9.3 Capitalization Threshold
All purchases of computers shall be capitalized, as there is no minimum dollar amount.

Approved by 8 members of the Finance Committee.

Adopted October 22, 2014 by voice vote.

ACT NO. 478-2014 by Mr. Snyder, Sr.
*and Mrs. Stockman*¹

**AUTHORIZING THE CHAIR TO EXECUTE CONTRACT WITH
SYSTEMS EAST, INC. FOR
APPLICATION SOFTWARE AND SUPPORT SERVICES FOR
REAL PROPERTY TAX MANAGEMENT**

Pursuant to Section 450 of the County Law.

WHEREAS, Act 497-2013 authorized a contract with Systems East, Inc., 6 Locust Avenue, Cortland, New York 13045, for the provision of application maintenance and support services for the Total Collection Solution (TCS.web) for an amount of \$21,276.00, the term of which expires December 31, 2014, and

WHEREAS, the Treasurer's Office is desirous of continuing annual application maintenance and support services, and

WHEREAS, Systems East, Inc., can provide application maintenance and support services for an amount of \$1,798.00 per month for a total contract amount of \$21,576.00, for the period January 1, 2015 through December 31, 2015, now, therefore, be it

RESOLVED, that the Chair of the Legislature be, and hereby is, authorized and directed to execute a contract, contingent upon and subject to inclusion in the 2015 budget of sufficient funds to cover the costs of the aforementioned services, on behalf of Cattaraugus County, with Systems East, Inc., for the provision of the above-described application maintenance and support services, for a term commencing January 1, 2015 and terminating December 31, 2015, according to the above-described terms.

Approved by 8 members of the Finance Committee and 7 members of the County Operations Committee.

¹The following Legislator requested her name be listed as an additional sponsor: "Mrs. Stockman".

Adopted October 22, 2014 by voice vote.

ACT NO. 479-2014 by Mr. Klancer, Mr. Marsh, Mr. McElfresh, Mrs. Stockman,
Mr. Teachman, Mr. Snyder, Jr., Mr. Weller,
Mr. Koch, Mrs. Labuhn, Mr. Padlo and Mr. Sprague

ADOPTION OF CATTARAUGUS COUNTY INFORMATION SECURITY POLICIES AND PROCEDURES

Pursuant to Section 153 of the County Law.

RESOLVED, that the following Cattaraugus County Information Security Policies And Procedures is hereby adopted by the Cattaraugus County Legislature:

Cattaraugus County Information Security Policies And Procedures

Table of Contents

Information Security and Accountability	564
Policy Monitoring and Enforcement	565
Organizational Security and Functional Responsibilities	566
Employee Information Security Policy Agreement	567
Acceptable Use Policies	568
CCIS- 0010.000 Policy - Email	568
CCIS- 0020.000 Policy - Telephony Services	571
CCIS- 0040.000 Policy - Mobile Devices.....	573
CCIS- 0050.000 Policy - Internet	575
CCIS- 0060.000 Policy – Printers and Copiers.....	577
CCIS- 0070.000 Policy – Social Networks.....	579
CCIS- 0080.000 Policy – Instant Messaging	580
Security Policies	581
CCIS- 0090.000 Policy – Network ID	581
CCIS- 0110.000 Policy – Removable Media	582
CCIS- 0120.000 Policy – Anti-Virus and Malware	584
CCIS- 0130.000 Policy – Third Party Access	585
CCIS- 0140.000 Policy – Security Breach Reporting.....	588
Communications and Network Management Policies	589
CCIS- 0150.000 Policy – Remote Access	589
CCIS- 0160.000 Policy – Wireless Networks	591
CCIS- 0190.000 Policy – Asset Disposal	593
CCIS- 0200.000 Policy – Software Use/Licensing.....	596
CCIS- 0220.000 Policy – Data Backups.....	597
Contact Information	598

Information Security and Accountability

Preface

The Information Security Policies and Procedures are a statement of the minimum requirements, ethics, responsibilities and accepted behaviors required to establish and maintain a secure environment, and achieve the County's acceptable use and information security objectives. Compliance with these policies, guidelines and procedures is expected and it is the responsibility of each County Department Head to ensure their departments are in compliance.

Purpose

The purpose of this document is to ensure the confidentiality, integrity, and availability of computing resources by defining a set of minimum policies, guidelines and procedures that outlines the appropriate use, acquisition, and implementation that all Cattaraugus County departments should strive to meet. This document applies to all Information Technology hardware, software, facilities, applications, and networks that are a part of Cattaraugus County's computing resources and shall serve as best practices for the County, inclusive of all campus locations. Any department may, based on its individual business needs and specific legal requirements such as the Health Insurance Portability and Accountability Act (HIPAA), exceed the guidelines put forth in this document, but should, at a minimum, achieve the security levels outlined herein.

Scope

These policies and procedures apply to all County departments but are not intended to unilaterally change the terms and conditions of employment. All County departments, when coming into compliance with these policies, guidelines and procedures, should consider all terms and conditions of employment as well as collective bargaining agreements.

These policies, guidelines and procedures are applicable to County departments, staff and all others, including outsourced third parties, which have access to or manage County information. Where conflicts exist between these policies, guidelines and procedures and a County department guideline, the more restrictive guideline should take precedence.

Policy Monitoring and Enforcement

Computing systems and resources provided by Cattaraugus County are owned by the County and are therefore its property. This gives Cattaraugus County the right to monitor any and all voice and data traffic passing through its system.

In addition, backup copies of voice or data traffic may exist, despite end-user deletion, in compliance with Cattaraugus County's records retention policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss.

If Cattaraugus County discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, voice or data records may be retrieved and used to document the activity in accordance with due process.

Reporting Misuse

Any allegations of misuse should be promptly reported to your Department Head and the Director of Information Services. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the individuals referenced above.

Disclaimer

Cattaraugus County assumes no liability for direct and/or indirect damages arising from an employee's use of Cattaraugus County's voice or data services. Employees are solely responsible for the content they disseminate. Cattaraugus County is not responsible for any third-party claim, demand, or damage arising out of use of the County's voice or data services.

Failure to Comply

Violations of any Information Technology Policy will be treated like other allegations of wrong doing at Cattaraugus County. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use on County voice or data services may include, but are not limited to, one or more of the following:

- Temporary or permanent revocation of access to voice or data resource;
- Disciplinary action up to and including termination of employment according to applicable County policies and/or Collective Bargaining Agreements;
- Legal action according to applicable laws and contractual agreements.

Organizational Security and Functional Responsibilities**Information Owners**

Cattaraugus County departments are considered the information owners for the data and tools they administer. Information owners are responsible for determining who should have access to protected resources within their department, and what those access privileges should be (read, update, delete, archive, etc.). These access privileges should be in accordance with the user's job responsibilities.

County Employees

It is the responsibility of all employees to protect County information and resources, including passwords, and to report suspected security incidents to the appropriate manager and the Director of Information Services. County employees are expected to adhere to the guidelines outlined in this document.

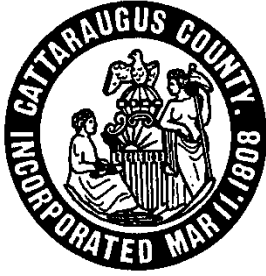
Non-County Employees

Individuals, who work under the agreements with the County such as Contractors, Consultants, Vendors, interns, volunteers and other persons in similar positions, to the extent of their present or past access to County information, are also covered by this Information Security Guidelines document.

Information Technology (IT)

Information Services management has responsibility for the data processing infrastructure, data, voice and wireless networks, that support the information owners. It is the responsibility of Information Services management to support these policies, guidelines and procedures and provide resources needed to enhance and maintain a level of information security control that is consistent with this document.

Information Services designated staff are responsible for the implementation of this and other acceptable use and information security guidelines, but the compliance of County employees to these policies, guidelines and procedures is the Department Head's responsibility. The designated staff should educate County employees with regard to acceptable use and information security issues. Staff should be made aware of why the guidelines have been established, and what role(s) individuals have in safeguarding information.

Employee Information Security Policy Agreement

My signature below indicates that I have been provided with a copy of the Cattaraugus County Information Security Policies and Procedures and I agree to abide by the policies and procedures explained herein. I understand it is my responsibility to read / review these policies and procedures and become familiar with them. If I violate any of the Information Security policies I may face legal or disciplinary action according to applicable laws, County policy, or within the applicable Collective Bargaining Agreement.

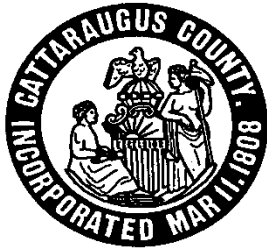
Employee Name (Printed)

Employee Signature

Date

Department

Acceptable Use Policies**CCIS- 0010.000 Policy - Email**



Title	Number
Policy - Acceptable Use of Email	CCIS-0010.000
Creation Date: October 2014	
Modified Date:	

Purpose: E-mail is a critical mechanism for business communications at Cattaraugus County. However, use of Cattaraugus County's electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of Cattaraugus County. The objectives of this policy are to outline appropriate and inappropriate use of Cattaraugus County's e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

Scope: This policy applies to all e-mail systems and services owned by Cattaraugus County, all e-mail account users/holders at Cattaraugus County (both temporary and permanent), and all County e-mail records.

General Policy: E-mail access at Cattaraugus County is controlled through individual accounts and passwords. It is the responsibility of the employee to protect the confidentiality of their account and password information.

Employees of Cattaraugus County are provided an e-mail account based on job function and business need as determined by the Department Head. E-mail accounts will be granted to third party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include:

- Contractors
- Research Partners
- Interns

E-mail access will be terminated when the employee or third party terminates his/her association with Cattaraugus County, unless other arrangements are made. Cattaraugus County is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

Important official communications are often delivered via e-mail. As a result, employees of Cattaraugus County with e-mail accounts are expected to check their e-mail so that they are aware of important County announcements and updates, as well as for fulfilling business- and role-oriented tasks.

E-mail users are responsible for mailbox management, including organization and cleaning. Email quota's are determined based on job functions and exist to control email storage costs and ensure the performance of the email application. Once your email quota is reached you must delete / archive email before the application will allow you to send any more email messages.

E-mail users are also expected to comply with normal standards of professional and personal courtesy and conduct.

Individuals at Cattaraugus County are encouraged to use e-mail to further the goals and objectives of Cattaraugus County. The types of activities that are encouraged include:

- Communicating with fellow employees, business partners of Cattaraugus County, and clients within the context of an individual's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Participating in educational or professional development activities.

Cattaraugus County's e-mail systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems. Individual e-mail use will not interfere with others' use of Cattaraugus County's e-mail system and services.

The following activities are deemed inappropriate uses of Cattaraugus County systems and services and are prohibited:

- Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- Use of e-mail in any way that violates Cattaraugus County's policies, rules, or administrative orders.
- Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user.
- Excessive personal use of Cattaraugus County e-mail resources. Cattaraugus County allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. Cattaraugus County prohibits personal use of its e-mail systems and services for unsolicited mass mailings, non-Cattaraugus County commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.

The e-mail systems and services used at Cattaraugus County are owned by the County, and are therefore its property. This gives Cattaraugus County the right to monitor any and all e-mail traffic passing through its e-mail system.

In addition, backup copies of e-mail messages may exist, despite end-user deletion, in compliance with Cattaraugus County's records retention policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss.

If Cattaraugus County discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, e-mail records may be retrieved and used to document the activity in accordance with due process.

Use extreme caution when communicating confidential or sensitive information via e-mail. Keep in mind that all e-mail messages sent outside of Cattaraugus County become the property of the receiver. A

good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "Reply" command during e-mail correspondence.

Any allegations of misuse should be promptly reported to your immediate supervisor. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the individual named above.

Cattaraugus County assumes no liability for direct and/or indirect damages arising from the user's use of Cattaraugus County's e-mail system and services. Users are solely responsible for the content they disseminate. Cattaraugus County is not responsible for any third-party claim, demand, or damage arising out of use the Cattaraugus County's e-mail systems or services.

CCIS- 0020.000 Policy - Telephony Services



Title	Number
Policy - Acceptable Use of Telephony Services	CCIS-0020.000
Creation Date: October 2014	
Modified Date:	

Purpose: Telephone communication is an essential part of the day-to-day operations of Cattaraugus County. Telephone and voicemail services are provided to employees in order to facilitate performance of work. The goal of this policy is to balance the business need for telephone and voicemail use with the costs involved.

Scope: This policy applies to all employees of Cattaraugus County, and all usage of County provided telephone, voicemail and fax services.

General Policy: As with all Cattaraugus County resources, the use of telephones, voicemail and fax services should be as cost effective as possible and in keeping with the best interests of the County. All employees must operate within the following basic policy guidelines. Further information on appropriate and inappropriate use follows this section.

- All telephones, telephone equipment, voicemail boxes, and messages contained within voicemail boxes are the property of Cattaraugus County.
- The Information Services Department is responsible for installation and repair of all County telephone equipment and administration of telephone and voicemail accounts with the exception of the Sheriff's Department e911 Dispatch Center. The Captain of Communications for the Sheriff's Department is accountable for this operation.
- Department supervisors are responsible for overseeing telephone and voicemail use and ensuring policy compliance, as well as ensuring IT is notified of any adds, moves, or changes required to telephone or voicemail services.
- Use of directory assistance (i.e. 411) should be avoided since a fee is incurred with each use. If you are unsure of a number, please consult online telephone directories first.

Unacceptable Use

Cattaraugus County telephone, voicemail or fax services may not be used for the following:

- Transmitting obscene, profane, or offensive messages.
- Transmitting messages or jokes that violate our harassment policy or create an intimidating or hostile work environment.
- Using the telephone system or breaking into a voicemail box via unauthorized use of a PIN or other password.

- Broadcasting unsolicited personal views on social, political, or other non-business related matters.
- Soliciting to buy or sell goods or services unrelated to Cattaraugus County.
- Making personal long-distance phone calls without supervisor permission.
- Misuse of telephone and voicemail services may result in disciplinary action, up to and including termination.

Limited Personal Acceptable Use

In general, personal use of telephone, voicemail or fax services is allowable, but must be limited in number and duration and must not interfere with performance of official business duties. Limited personal acceptable use is allowed.

Monitoring

Cattaraugus County reserves the right to monitor telephone, voicemail and fax use, including telephone conversations and the contents of voicemail boxes. Monitoring of telephone and voicemail use will only be done for legitimate reasons, such as to assess customer service quality assurance, retrieve lost messages, recover from system failure, or comply with investigations of wrongful acts.

CCIS- 0040.000 Policy - Mobile Devices



Title	Number
Policy - Acceptable Use of Mobile Devices	CCIS-0040.000
Creation Date: October 2014	
Modified Date:	

Purpose: The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of Cattaraugus County's direct control. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/netbook/tablet computers.
- Mobile/cellular phones, air cards and GPS devices.
- Smartphones, Blackberry's, etc.
- Home or personal devices used to access corporate resources.
- Any mobile device capable of storing corporate data and connecting to an unmanaged network.

Scope: The policy applies to any hardware and related software that could be used to access corporate resources, even if said equipment is not corporately sanctioned, owned, or supplied.

The overriding goal of this policy is to protect the integrity of the private and confidential client and business data that resides within Cattaraugus County's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the County's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Cattaraugus County's direct control to backup, store, and otherwise access corporate data of any type must adhere to County-defined processes for doing so.

This policy applies to all Cattaraugus County employees, including full and part-time staff, contractors, freelancers, and other agents who utilize either County-owned or personally-owned mobile device to access, store, back up, relocate or access any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust the County has built with its clients, supply chain partners and other constituents. Consequently, employment at Cattaraugus County does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

Connectivity of all mobile devices will be centrally managed by Cattaraugus County's IT department and will utilize authentication and strong encryption measures. Although IT is not able to directly manage

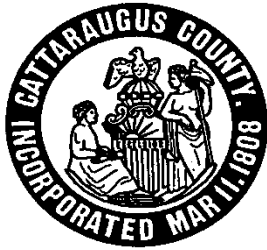
external devices – such as home PCs – which may require connectivity to the corporate network, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the County's infrastructure.

General Policy: It is the responsibility of any employee of Cattaraugus County who uses a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct County business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

Based on this, the following rules must be observed:

- IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to the County infrastructure. IT will engage in such action if it feels equipment is being used in such a way that puts the County's systems, data, or users at risk.
- End users who wish to connect such devices to non-county network infrastructure to gain access to County data **must employ**, for their devices and related infrastructure, **a County-approved personal firewall** and any other security measure deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet Cattaraugus County's established enterprise IT security standards.
- Laptop computers or personal PCs may only access the corporate network and data using a Virtual Private Network (VPN) or Remote Desktop Services (RDS) connection. The SSL VPN portal Web address will be provided to users as required.
- All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by Cattaraugus County's IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.
- In the event of a lost or stolen mobile device it is incumbent on the user to report this to IT immediately. The device will be remotely wiped of all data and locked if possible to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.

CCIS- 0050.000 Policy - Internet



Title	Number
Policy - Acceptable Use of the Internet	CCIS-0050.000
Creation Date: October 2014	
Modified Date:	

Purpose: The goals of this policy are to outline appropriate and inappropriate use of Cattaraugus County's Internet resources.

Scope: Internet access at Cattaraugus County is controlled through individual user accounts and passwords. Department managers are responsible for defining appropriate Internet access levels for the people in their department and conveying that information through a Help Desk Service Request ticket to the IT Help Desk.

General Policy:

Appropriate Use: Employees at Cattaraugus County are encouraged to use the Internet to further the goals and objectives of Cattaraugus County. The types of activities that are encouraged include:

- Utilization of online applications directly related to job responsibilities;
- Acquiring information necessary or related to the performance of an individual's assigned responsibilities; and
- Participating in educational or professional development activities.

Inappropriate Use: Individual Internet use will not interfere with others' productive use of Internet resources. Internet use at Cattaraugus County will comply with all Federal and New York State laws, all Cattaraugus County policies, and all Cattaraugus County contracts. This includes, but is not limited to, the following:

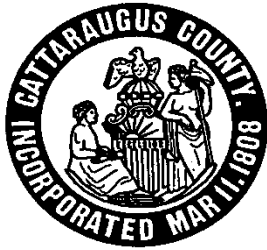
- The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, sexual harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, prohibited discriminatory activity, disruptive, unethical, unprofessional behavior and computer tampering (e.g. spreading computer viruses).
- The Internet may not be used in any way that violates Cattaraugus County's policies, rules, or administrative orders. Use of the Internet in a manner that is not consistent with the mission of Cattaraugus County, misrepresents Cattaraugus County, or violates any Cattaraugus County policy is prohibited.

- Cattaraugus County's Internet Services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems. Individual internet use will not interfere with others' use of Cattaraugus County's Internet Services.
- Cattaraugus County prohibits uploading and downloading of files for personal use, and access to categories of sites (pornography, gaming, streaming media, etc.) as defined by access levels.
- Individuals may not establish County computers as participants in any peer-to-peer network file sharing programs, file transfer programs, Bittorrent programs (e.g. Gnutella, Kazaa, Morpheus, Audiogalaxy, BearShare, LimeWire, iMesh, WinMX, Madster, BITcoin) or listservs running on County information systems without consent from the Director of IS. Users shall not install internet software or programs unless authorized by the Director of IS or designee. Any unauthorized internet downloaded programs will be subject to removal by IT staff upon detection.
- Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to Cattaraugus County or another individual without authorized permission.

Security: For security purposes, users may not share account or password information with another person. Internet accounts are to be used only by the assigned user of the account for authorized purposes. Attempting to obtain another user's account password is strictly prohibited. A user must contact the help desk or IT administrator to obtain a password reset if they have reason to believe that any unauthorized person has learned their password. Users must take all necessary precautions to prevent unauthorized access to Internet services.

Monitoring and Filtering: Cattaraugus County may monitor any Internet activity occurring on Cattaraugus County equipment or accounts. Cattaraugus County currently does employ filtering software to limit access to sites on the Internet. If Cattaraugus County discovers activities which do not comply with applicable law or departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

CCIS- 0060.000 Policy – Printers and Copiers



Title	Number
Policy – Acceptable Use of Printers and Copiers	CCIS-0060.000
Creation Date: October 2014	
Modified Date:	

Purpose: Printers and copiers represent one of the highest equipment expenditures at Cattaraugus County. The goal of this policy is to facilitate the appropriate and responsible business use of printer and copier assets, as well as control these cost of ownership by preventing the waste of paper, toner, ink, and so on.

Scope: This Printer and Copier Policy applies to all employees of Cattaraugus County as well as any contract employees in the service of the County who may be using this equipment.

General Policy:

- Printers and copiers are to be used for documents that are relevant to the day-to-day conduct of business at Cattaraugus County. Printers and copiers should not be used to print personal documents.
- Installation of personal printers is generally not condoned at Cattaraugus County due to the cost of maintaining and supporting many dispersed machines. In certain circumstances, however, where confidentiality, remote location, the need to print a large number of low volume print jobs, or other unusual situation is at issue, personal printers may be allowed.
- Do not print multiple copies of the same document – the printer is not a copier and typically costs more per page to use. If you need multiple copies, print one good copy on the printer and use the copier to make additional copies or send the entire output to a networked attached copier.
- If you print something to a common network attached printer / copier, please pick it up in a timely fashion. If you no longer want it, please dispose of it appropriately (i.e. recycle).
- Make efforts to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing) features offered by some printers / copiers and other optimization features (e.g. printing six PowerPoint slides per page versus only one per page).
- Make efforts to limit toner use by selecting light toner and lower dpi default print settings.
- Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer / copier. If printing a job in excess of 25 pages, please be at the printer to collect it when it comes out to ensure adequate paper supply for the job and that the output tray is not overfull (i.e. you may need to remove some of the output before the print job is finished).

- Avoid printing e-mail messages. This is wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.
- Avoiding printing a document just to see what it looks like. This is wasteful.
- Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult with IT to find out which machines can handle these specialty print jobs.
- Color printing is typically not required by general business users. Given this selective need, as well as the high cost per page to print color copies, the number of color-capable printers available has been minimized. You are strongly encouraged to avoid printing in color when monochrome (black) will do.
- If you encounter a physical problem with the printer / copier (paper jam, out of toner, etc.) and are not “trained” in how to fix the problem, please do not try. Instead, report the problem to the IT Help Desk or ask a trained co-worker for help.
- Report any malfunction of any printing device to the IT Help Desk as soon as possible.

CCIS- 0070.000 Policy – Social Networks



Title	Number
Policy – Acceptable Use of Social Networks	CCIS-0070.000
Creation Date:	October 2014
Modified Date:	

Purpose: Social networking and other Web 2.0 technologies can help support Cattaraugus County business purposes. However, improper uses of such technologies raise security and network performance risks and the potential for damage to the County’s technology resources. The objective of this policy is to outline appropriate and inappropriate use of Social networking and other Web 2.0 technologies in order to minimize disruptions to services and activities.

Scope: This policy applies to all social networking and Web 2.0 technologies including but not limited to Facebook, MySpace, Twitter and LinkedIn that are accessed using a Cattaraugus County email address, network access ID, or personal ID. Employees are responsible for their online activities that are conducted with any of these personal identities.

Employees should be aware that all Cattaraugus County Policies related to harassment, bullying, workplace violence, and ethics extend to all forms of communication (including social networking media) both inside and outside the workplace.

General Policy: A Cattaraugus County employee may only use social networking or Web 2.0 technologies if authorized by his or her Department Head and the Director of Information Technology. Otherwise, accessing social networking or Web 2.0 technologies from a Cattaraugus County computer is prohibited.

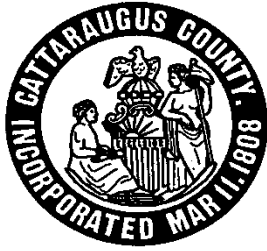
Appropriate Use: Upon approval, individuals are able to utilize social networking or Web 2.0 technologies to further the goals and objectives of Cattaraugus County. The types of activities that are encouraged include:

- Creation and monitoring of a social networking presence for a particular department such as the Health Department; and
- Accessing social networking sites to gather information critical to public safety.

Inappropriate Use: Individuals shall not divulge sensitive or private information related to County operations or clients of any department whether operating on County sites, or personal sites. The types of activities that are forbidden include:

- Posting any information in violation of Federal, State, or County policies including (but not limited to) HIPAA, Identity Protection, and Workplace Violence. This applies whether the employee is utilizing a County account or a personal account.
- Divulging names, addresses, or other status or contact information about any County employee without consent of that employee, or any client of County services at any time.

CCIS- 0080.000 Policy – Instant Messaging



Title	Number
Policy – Acceptable Use of Instant Messaging	CCIS-0080.000
Creation Date: October 2014	
Modified Date:	

Purpose: Instant Messaging (IM) is currently being used by Cattaraugus County as a form of real-time communication with individuals inside the organization. IM technology is meant for the purpose of enhancing employee productivity while conducting Cattaraugus County business. However, IM carries some security risks that must be addressed.

The use of IM at Cattaraugus County is a privilege and its abuse or misuse will not be tolerated. It is the responsibility of the IT department to ensure that IM is supported. It is the responsibility of the user to exercise sound judgment and common sense while using IM to fulfill his or her job duties.

Scope: This policy applies to all IM use at Cattaraugus County inclusive of all locations. This policy applies to all County employees, including full-time, part-time, contractors, interns, consultants, suppliers, and other third parties.

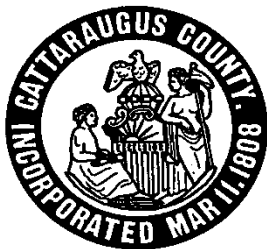
General Policy: Cattaraugus County has selected Lotus Notes Sametime as its sole provider of corporate IM services. Non-sanctioned IM services could affect network security, so the corporate firewall has been configured to block them. Free IM services commonly used within the consumer market are NOT approved or supported by the IT department.

IM services are to be used for business communications and for the purpose of fulfilling job duties, in accordance with County goals and objectives and it is expected that all employees will communicate professionally at all times.

Instant messages are considered business records and fall under certain compliance rules and regulations. As such, IM discussions are subject to existing policies and procedures regarding business record retention, storage, and deletion.

Security Policies

CCIS- 0090.000 Policy – Network ID



Title	Number
Policy – Network ID and Password	CCIS-0090.000
Creation Date:	October 2014
Modified Date:	

Purpose: Passwords are an important component of information and network security. The use of a Network-ID and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used and protected appropriately to ensure that the level of security they imply is actually met. The purpose of this policy is to provide the guidelines necessary for all of the employees of Cattaraugus County to create appropriate passwords and to use them and protect them in an appropriate manner.

Scope: This policy applies to all employees of Cattaraugus County who have any form of computer or application account that requires password access.

General Policy:

- Password construction, lifecycle and re-use parameters will be variable according to the application that they are intended to protect.
- Passwords should not be based on well-known or easily accessible information, including personal information, nor should they be words commonly found within a standard dictionary.
- Users will be notified in advance of county password expiration. At that point, and at every subsequent login until a change is made, users will be prompted to select a new password.
- Strong password construction is required and needs to adhere to the current password standards.
- Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at their password to another person, including administrators, superiors, other co-workers, friends, and family members.
- No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe or desk drawer if in hardcopy form or in an encrypted file if in electronic form.
- Each employee is responsible for all transactions made using his/her password.
- The IT Department may attempt to crack or guess users passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

CCIS- 0110.000 Policy – Removable Media



Title	Number
Policy – Removable Media	CCIS-0110.000
Creation Date: October 2014	
Modified Date:	

Purpose: The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to connect portable removable media to any infrastructure within Cattaraugus County's internal network(s) or related technology resources. This removable media policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.
- Memory cards in SD, CompactFlash, Memory Stick, or any related flash-based supplemental storage media.
- USB card readers that allow connectivity to a PC.
- Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function.
- PDAs, cell phone handsets, and Smartphone's with internal flash or hard drive-based memory that support a data storage function.
- Digital cameras with internal or external memory support.
- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.
- Any hardware that provides connectivity to USB devices through means such as wireless (WiFi, WiMAX, IrDA, Bluetooth, among others) or wired network access.

Scope:

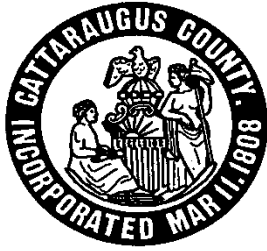
The policy applies to any hardware and related software that could be used to access County resources, even if said equipment is not corporately sanctioned, owned, or supplied.

General Policy: It is the responsibility of any employee of Cattaraugus County who is connecting a USB-based memory device to the organizational network to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any portable memory that is used to conduct Cattaraugus County business be utilized appropriately, responsibly, and ethically.

Based on this, the following rules must be observed:

-
- IT reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to corporate and corporate-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the County's systems, data, users, and clients at risk.
 - End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain County data. Any non-corporate computers used to synchronize with these devices will have installed up-to-date anti-virus and anti-malware software.
 - Passwords and other confidential data as defined by Cattaraugus County's IT department are not to be stored on portable storage devices.
 - Cattaraugus County's IT department will support sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media. This applies even to devices already known to the IT department.
 - IT reserves the right to physically disable USB ports to limit physical and virtual access and reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

CCIS- 0120.000 Policy – Anti-Virus and Malware



Title	Number
Policy – Anti-Virus and Malware	CCIS-0120.000
Creation Date: October 2014	
Modified Date:	

Purpose: A virus or malware is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses or malware can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, USB drives, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus or malware infection can be very costly to Cattaraugus County in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of Cattaraugus County is to provide a computing network that is virus and malware free. The purpose of this policy is to provide instructions on measures that must be taken by Cattaraugus County employees to help achieve effective virus and malware detection and prevention.

Scope: This policy applies to all computers that are connected to the Cattaraugus County network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both County-owned computers and personally-owned computers attached to the County's network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, smart phones and servers.

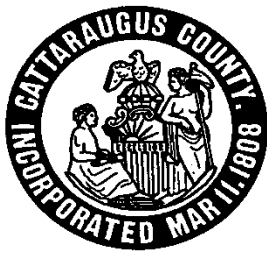
General Policy: All computers attached to the County's network must have approved anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

Any activities with the intention to create and/or distribute malicious programs onto the County network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

If an employee receives what he/she believes to be a virus or malware, or suspects that a computer is infected with a virus, he/she must contact the IT department immediately and report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT department.

Any virus or malware infected computer will be removed from the network until it is verified as virus or malware free.

CCIS- 0130.000 Policy – Third Party Access



Title	Number
Policy – Third Party Access	CCIS-0130.000
Creation Date: October 2014	
Modified Date:	

Purpose: The purpose of the Cattaraugus County Third-Party Access Policy is to establish the rules for third-party access to County information systems, third-party responsibilities, and protection of Cattaraugus County information.

Scope: The Cattaraugus County Third-Party Access Policy outlines responsibilities and expectations of any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. This policy also outlines the responsibilities and expectations of the County personnel responsible for the contracting and/or supervising of the third party. A third party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and security companies.

General Policy:

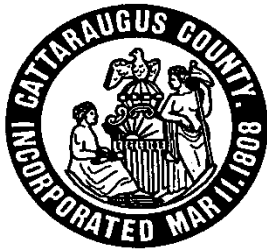
Information Systems Third-Party Policy Guidelines

- Any third-party agreements and contracts must specify:
- The work that is to be accomplished and work hours. Also, any configuration information of any installed software as well as virus checking of that software.
- The information that the third party requires access to.
- The minimum security requirements that the third party must meet (i.e. method for remote access).
- How County information is to be guarded by the third party. Signing of a non-disclosure agreement is required.
- Strict use of County information and information resources for the purpose of the business agreement by the third party. Any other County information acquired by the third party in the course of the contract cannot be used for the third-party's own purposes or divulged to others.
- Feasible methods for the destruction, disposal, or return of County information at the end of the contract.
- The return of County property such as a laptop, PDA, or cell phone after the completion or termination of the agreement.
- The third party must comply with all applicable Cattaraugus County standards, agreements, practices and policies, including, but not limited to:

- Acceptable use policies.
 - Software licensing policies.
 - Safety policies.
 - Auditing policies.
 - Security policies.
 - Non-disclosure policies.
 - Privacy policies.
-
- Cattaraugus County will provide an IT point of contact for the third party whether it is one person from the IT department or an interdepartmental team. This point of contact will liaise with the third party to ensure they are in compliance with these policies.
 - The third party will provide the County with a list of all additional third parties working on the contract. The list must be updated and provided to the County within 8 hours of any staff changes.
 - Third party access to systems must be uniquely identifiable and authenticated, and password management must comply with the Cattaraugus County Password Policy. Managing connectivity with partner networks can be handled different ways depending on what technologies are in place (i.e. encryption, intrusion detection, DMZ architecture).
 - Any third party computer/laptop/PDA/tablet PC that is connected to County systems must have up-to-date virus protection and patches. The third party will be held accountable for any damage occurred to the County in the event that an incident occurs.
 - Each third-party employee that has access to Cattaraugus County sensitive information should be cleared to handle that information.
 - If applicable, an explanation of how Cattaraugus County information will be handled and protected at the third party's facility/site must be addressed.
 - Third-party employees must report all security incidences to the appropriate County Information Services Department personnel.
 - If third-party management is involved in Cattaraugus County security incident management, the responsibilities and details must be specified in the contract.
 - The third party must follow all applicable change control procedures and processes.
 - All software used by the third party in providing service to Cattaraugus County must be properly inventoried and licensed.
 - All third-party employees are required to comply with all applicable auditing regulations and County auditing requirements, including the auditing of the third-party's work.
 - Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by the appropriate County Department management.
 - All third-party maintenance equipment on the County network that connects to the outside world via telephone lines, leased line, or the network will remain disabled except when in use for authorized maintenance.
 - The third party's major accomplishments must be documented and available to County management upon request. Documentation should include, but is not limited to events such as:

- Personnel changes.
 - Password changes.
 - Project milestones.
 - Deliverables.
 - Arrival and departure times.
- Upon departure of the third party from the contract for any reason, the third party will ensure that all sensitive information is collected and returned to the County or destroyed within 72 hours. The third party will also provide written certification of that destruction within 5 business days. All equipment and supplies must also be returned, as well as any access cards and identification badges. All equipment and supplies retained by the third party must be documented by authorized County management.

CCIS- 0140.000 Policy – Security Breach Reporting



Title	Number
Policy – Security Breach Reporting	CCIS-0140.000
Creation Date: October 2014	
Modified Date:	

Purpose: To protect the confidentiality of ‘personal or private information’ and provide direction for staff if they discover this data is inadvertently or intentionally disclosed.

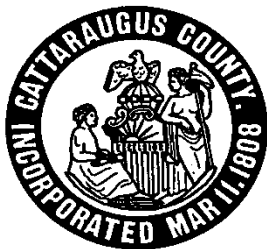
Scope: A compromise of personal or private information shall mean the unauthorized acquisition of unencrypted electronic data containing this information. If encrypted data is compromised along with the corresponding encryption key, the data shall be considered unencrypted and thus fall under this policy requirements.

General Policy: If it has been determined or is reasonably believed that private or personal information has been disclosed, the staff is directed to notify their immediate supervisor who in turn is to notify the County Attorney’s Office.

The County Attorney is responsible for determining the appropriate course of action for notification and disclosure.

Communications and Network Management Policies

CCIS- 0150.000 Policy – Remote Access



Title	Number
Policy – Remote Access	CCIS-0150.000
Creation Date:	October 2014
Modified Date:	

Purpose: The purpose of this policy is to define standards, procedures, and restrictions for connecting to Cattaraugus County’s internal network(s) from external hosts via remote access technology, and/or for utilizing the Internet for business purposes via third-party wireless Internet service providers (a.k.a. “hotspots”). Cattaraugus County’s resources (i.e. county data, computer systems, networks, databases, etc.) must be protected from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all remote access and mobile privileges for County employees to enterprise resources – and for wireless Internet access via hotspots – must employ only County-approved methods.

Scope: This policy applies to all Cattaraugus County employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who utilize County- or personally-owned computers to remotely access the organization’s data and networks. Employment at Cattaraugus County does not automatically guarantee the granting of remote access privileges.

Any and all work performed for Cattaraugus County on said computers by any and all employees, through a remote access connection of any kind, is covered by this policy. Work can include (but is not limited to) e-mail correspondence, Web browsing, utilizing intranet resources, and any other County application used over the Internet. Remote access is defined as any connection to the County’s network and/or other applications from off-site locations, such as the employee’s home, a hotel room, airports, cafés, satellite office, wireless devices, etc.

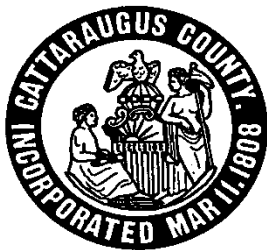
All remote access will be centrally managed by Cattaraugus County’s Information Services department and will utilize encryption and strong authentication measures. Remote access connections covered by this policy include (but are not limited to) Internet dial-up modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, proprietary remote access/control software, etc.

Employees may use privately owned connections for business purposes. If this is the case, the IT department must approve the connection as being secure and protected. However, the County’s IT department cannot and will not technically support a third-party ISP connection or hotspot wireless ISP connection. All expense forms for reimbursement of cost (if any) incurred due to remote access for business purposes (i.e. Internet connectivity charges) must be submitted to the appropriate unit or department head. Financial reimbursement for remote access is not the responsibility of the IT department.

General Policy: It is the responsibility of any employee of Cattaraugus County with remote access privileges to ensure that their remote access connection remains as secure as his or her network access within the office. It is imperative that any remote access connection used to conduct Cattaraugus County business be utilized appropriately, responsibly, and ethically. Therefore, the following rules must be observed:

- Employees will use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with the County's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
- All remote computer equipment and devices used for business interests, whether personal- or County-owned, must display reasonable physical security measures. Computers will have installed whatever antivirus software deemed necessary by Cattaraugus County's IT department.
- Remote users using public hotspots for wireless Internet access must employ for their devices a County-approved personal firewall, VPN, and any other security measure deemed necessary by the IT department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with Cattaraugus County's additional security measures.
- Hotspot and remote users must disconnect wireless cards when not in use in order to mitigate attacks by hackers, wardrivers, and eavesdroppers.
- Any remote connection (i.e. hotspot, ISDN, frame relay, etc.) that is configured to access Cattaraugus County resources must adhere to the authentication requirements of the County's IT department. In addition, all hardware security configurations (personal or County-owned) must be approved by Cattaraugus County's IT department.
- Employees, contractors, and temporary staff will make no modifications of any kind to the remote access connection without the express approval of the County's IT department. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware or security configurations, etc.
- Employees, contractors, and temporary staff with remote access privileges must ensure that their computers are not connected to any other network while connected to Cattaraugus County's network via remote access, with the obvious exception of Internet connectivity.
- In order to avoid confusing official County business with personal communications, employees, contractors, and temporary staff with remote access privileges must never use non-County e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct Cattaraugus County business.
- If a personally- or County-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized user will be responsible for notifying their manager and Cattaraugus County's IT department immediately.
- The remote access user also agrees to immediately report to their manager and the County's IT department any incident or suspected incidents of unauthorized access and/or disclosure of County resources, databases, networks, etc.
- The remote access user also agrees to and accepts that his or her access and/or connection to Cattaraugus County's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

CCIS- 0160.000 Policy – Wireless Networks



Title	Number
Policy – Wireless Networks	CCIS-0160.000
Creation Date: October 2014	
Modified Date:	

Purpose: The purpose of this policy is to outline appropriate and inappropriate use of Cattaraugus County's Wireless Networking resources, including:

- Devices that are permitted to connect to the wireless network;
- Standards for hardware and software that will be used;
- Access privileges for the wireless network (i.e. who is authorized and who is not authorized to use the wireless network);
- Required security measures (including user passwords and how frequently they must be changed);
- Appropriate use of County assets (e.g. e-mail, Internet access); and
- Consequences for violating the wireless networking policy.

Scope: Only County owned and approved wireless devices maybe connected to the wireless network. The IT department is responsible for approving wireless devices for use on the network. In certain situations, non-county owned devices may be permitted to connect to the wireless network (e.g. customer PDAs, suppliers connecting to County-owned printers through the wireless network). The IT department must approve each of these situations in advance.

General Policy: The IT department is responsible for setting standards for hardware, software, and other technology that will be used in the wireless network. Only the Information Services Department is authorized to attach wireless hubs or switches (commonly known as Access Points or AP's) to the Cattaraugus County cabled network.

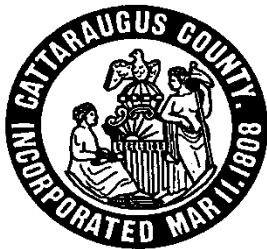
User-owned equipment will not necessarily be in compliance with corporate standards, and may not be supported by the IT department. Users should contact the IT department to discuss any issues relating to wireless networking technology standards.

The IT department is responsible for granting access privileges to the wireless network. To grant specific users access to the wireless network, department managers should contact the IT department and make a formal request. This request should include specific users who need wireless networking access, the wireless devices they will use, the locations they will connect to the wireless network, and other information that the IT department may need to set up the wireless access.

All users accessing the wireless network must comply with County security policies. These policies include using network-access passwords, regularly changing these passwords, using encrypted connections, and other policies required by the IT department.

Users are expected to secure their machines when they are using wireless network services. Computers must have active antivirus software. Antivirus signature files and operating system security patches must be kept up to date.

CCIS- 0190.000 Policy – Asset Disposal



Title	Number
Policy – Asset Disposal	CCIS-0190.000
Creation Date: October 2014	
Modified Date:	

Purpose: The purpose of this policy is to establish and define standards, procedures, and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner. Cattaraugus County's surplus or obsolete IT assets and resources (i.e. desktop computers, servers, cell phone's etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents. Therefore, all disposal procedures for retired IT assets must adhere to County-approved methods.

Scope: This policy applies to the proper disposal of all non-leased Cattaraugus County IT hardware, including PCs, printers, handheld devices, servers, hubs, switches, bridges, routers and cell phones. County-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by this policy. Where assets have not reached end of life, it is desirable to achieve some residual value of the IT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function.

Definitions:

- Non-leased refers to any and all IT assets that are the sole property of Cattaraugus County; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or partner company.
- Disposal refers to the reselling, reassignment, recycling, donating, or throwing out of IT equipment through responsible, ethical, and environmentally sound means.
- Obsolete refers to any and all equipment over 10 years old and/or that which no longer meets requisite functionality.
- Surplus refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.
- Beyond reasonable repair refers to any and all equipment whose condition requires fixing or refurbishing that is likely cost equal to or more than total replacement.
- Disposal and disposal procedures of all IT assets and equipment will be centrally managed and coordinated by Cattaraugus County's IT department. Cattaraugus County's IT department is also responsible for backing up and then wiping clean County data on all IT assets slated for disposal, as well as the removal of County tags and/or identifying labels. The IT department is in charge of selecting and approving external agents for recycling hardware and/or sanitizing hardware of harmful toxins before shipment to landfills. The IT department is also responsible for acquiring credible documentation from third parties that are contracted to conduct the data wiping, tag or label removal, or any other part of the disposal process.

Acceptable methods for the disposal of IT assets are as follows:

- Sold as scrap to a licensed dealer;
- Used as trade-in against cost of replacement item;
- Reassigned to a less critical business operation function;
- Recycled and/or refurbished to leverage further use (within limits of reasonable repair); and
- Discarded by a licensed and approved service provider in accordance with all local, state and federal laws.

General Policy: It is the responsibility of Cattaraugus County's IT department with the appropriate authority to ensure that IT assets, equipment, and hardware are disposed of according to one or more of the methods prescribed above.

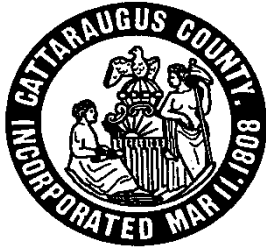
It is imperative that any disposals performed by Cattaraugus County are done appropriately, responsibly, and ethically, as well as with County resource planning in mind. **The disposal, sale or gifting of any County owned asset requires the written approval of the County Legislature in the form of an adopted resolution.**

The following rules must therefore be observed:

- **Obsolete IT Assets:** As prescribed above, "obsolete" refers to any and all computer or computer-related equipment over 10 years old and/or equipment that no longer meets requisite functionality. Identifying and classifying IT assets as obsolete is the sole province of the County's IT department. Decisions on this matter will be made according to Cattaraugus County's purchasing/procurement strategies. Equipment lifecycles are to be determined by IT asset management best practices (i.e. total cost of ownership, required upgrades, etc.).
- **Reassignment of Retired Assets:** Reassignment of computer hardware to a less-critical role is made at the sole discretion of the County's IT department. It is, however, the goal of Cattaraugus County to – whenever possible – reassign IT assets in order to achieve full return on investment (ROI) from the equipment and to minimize hardware expenditures when feasible reassignment to another business function will do instead.
- **Trade-Ins:** Where applicable, cases in which a piece of equipment is due for replacement by a newer model, reasonable actions must be taken to ensure that a fair and market trade-in value is obtained for the old IT asset against the cost of the replacement. Cattaraugus County's Purchasing and Procurement Director or IT Asset manager will assume this responsibility.
- **Cannibalization and Assets Beyond Reasonable Repair:** The IT Director is responsible for verifying and classifying any IT assets beyond reasonable repair. Equipment identified as such should be cannibalized for any spare and/or working parts that can still be put to sufficient use within the organization. The IT department will inventory and stockpile these parts. Remaining parts and/or whole machines unfit for use or any other disposal means will be sold to an approved scrap dealer or salvaging company.
- **Decommissioning of Assets:** All hardware slated for disposal by any means must be fully wiped clean of all County data. The County's IT department will assume responsibility for decommissioning this equipment by deleting all files, County-licensed programs, and applications using a pre-approved disk-sanitizer. This sanitizer must **completely overwrite** each and every disk sector of the machine with zero-filled blocks. In addition, any property tags or identifying labels must also be removed from the retired equipment.

-
- **Harmful Substances:** Hazardous materials such as lead, mercury, bromine, cadmium, etc. must be thoroughly removed from computer hardware before shipment to a landfill as rubbish. The IT department may perform this action itself using government-approved disposal methods, or hire an accredited disposal County specializing in this service. No matter what the route taken, the removal and discarding of toxins from County equipment must be in full compliance with local and federal laws.

CCIS- 0200.000 Policy – Software Use/Licensing



Title	Number
Policy – Software Use/Licensing	CCIS-0200.000
Creation Date: October 2014	
Modified Date:	

Purpose: Cattaraugus County believes in respecting and protecting the rights of intellectual property owners. This is not only a question of ethics, but also of law. Advances in electronic communication and technology, such as the Internet, have had a dramatic impact on the way Cattaraugus County conducts business, and have greatly facilitated our access to a wide range of information and media including software programs and downloaded programs from the internet. As a result, the risk of copyright infringement, either intentional or accidental, is of increasing concern.

Scope: The goal of this policy is to inform employees at Cattaraugus County on rules and procedures relating to copyright law compliance and valid licensing, and pertains to any and all County owned equipment and resources that are connected to the County network.

General Policy:

- Cattaraugus County reserves the right to monitor end-user systems and the content stored therein. Cattaraugus County also reserves the right to remove, delete, modify, or otherwise disable access to any materials found to be infringing on copyright, valid licensing or unauthorized installations or downloads.
- By reading and signing a copy of this policy, an employee of Cattaraugus County will indemnify and hold Cattaraugus County harmless for any breach of this policy or copyright law.
- No employee of Cattaraugus County may reproduce any copyrighted work in violation of the law. Unauthorized copying material includes but is not limited to, digitization, graphics, distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, mp3s or movies, logos, and the installation of any "pirated" or other copyrighted or unlicensed software products for which the County does not have an active appropriate license, is strictly prohibited. All software acquired must be reviewed and purchased through the Information Services Department. Under no circumstances will personal or unsolicited software be loaded onto County computers. Users are not permitted to bring software from home (or any other external source) and load it onto County computers. Users are not permitted to install programs from the internet, including freeware or shareware unless reviewed and authorized by the County Information Services Department. Every piece of software is required to have a license and Cattaraugus County will not condone the use of any software that is not licensed. Unauthorized changes to software must not be made. Copying and reproducing County owned or licensed software for personal use is strictly prohibited.

CCIS- 0220.000 Policy – Data Backups



Title	Number
Policy – Data Backups	CCIS-0220.000
Creation Date: October 2014	
Modified Date:	

Purpose: This policy refers to the system level back up and retention of data that resides on Cattaraugus County servers and storage area networks. All Information Technology managed servers and storage area networks regardless of location are covered by this policy.

Scope: The data stored on the backup media referred to in this policy are primarily for Disaster Recovery purposes. Application level backup's that are used to recover from an application error or data corruption are not included in this policy.

This policy pertains to data stored on County supported servers and does not refer to backing up of data that resides on individual PC or notebook hard drives. **Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user.** It is strongly encouraged that end users save their data to the appropriate network drive in order that their data is backed up regularly in accordance with this policy.

In addition, files that are left open at the time the backup procedure is initiated may not be backed up. End users are reminded to save and close all files, as well as all related applications at the end of each work day.

General Policy: The backup and retention of information stored on County supported servers is the responsibility of the Information Services department. Full system backups will be performed once a week and incremental / differential (changed data) backups will be performed on the remaining days of the week.

Contact Information

Questions concerning this guideline or requests for changes may be directed to:
Director of Information Services
Information Services Department
Cattaraugus County
County Building
303 Court Street
Little Valley, New York 14755
716-938-2208

Approved by 8 members of the Finance Committee and 7 members of the County Operations Committee.

Adopted October 22, 2014 by voice vote.

ACT NO. 480-2014 by Mr. Teachman

**AUTHORIZING THE CHAIR TO EXECUTE CONTRACT WITH
VISION SOLUTIONS, INC. FOR SOFTWARE MAINTENANCE SERVICES**

Pursuant to Section 450 of the County Law.

WHEREAS, Act 290-2011, as amended, authorized a contract with Vision Solutions, Inc., for the provision of software maintenance for the replication of the Sheriff's Office production IBM AS400 System located at 303 Court Street in Little Valley, to the Sheriff's target (backup) IBM AS400 System located at the Public Works Facility in Little Valley, the term of which expires November 30, 2014, and

WHEREAS, the County Department of Information Services is desirous of renewing the aforementioned annual software maintenance, and

WHEREAS, Vision Solutions, Inc., Department CH19317, Palatine, Illinois 60055-9317, can provide the software maintenance necessary for the aforementioned replication of the IBM AS400 for an amount of \$7,454.16, to be paid as invoiced, for the term December 1, 2014 through November 30, 2015, and

WHEREAS, sufficient funds are included in the budget to cover the cost of the aforementioned services, now, therefore, be it

RESOLVED, that the Chair of the Legislature be, and hereby is, authorized and directed to execute a contract, on behalf of Cattaraugus County, with Vision Solutions, Inc., for the provision of the above-described software maintenance, for a term commencing December 1, 2014 and terminating November 30, 2015, according to the above-described terms.

Approved by 8 members of the Finance Committee, 7 members of the County Operations Committee and 7 members of the Public Safety Committee.

Adopted October 22, 2014 by voice vote.

ACT NO. 481-2014 by Mr. Murphy

**ADJUSTING VARIOUS APPROPRIATION AND REVENUE ACCOUNTS FOR
2014 STATE HOMELAND SECURITY PROGRAM
(Sheriff's Office)**

Pursuant to Public Law 107-56, Department of Homeland Security
Appropriations Act of 2005, Public Law 108-334 and
Sections 363, 366 and 450 of the County Law.

WHEREAS, Act 245-2014 authorized the Chairman to execute grant documents with the New York State Office of Homeland Security for the fiscal year 2014 State Homeland Security Program, and

WHEREAS, the County has been awarded an amount of \$40,000.00 under the fiscal year 2014 State Homeland Security Program, and

WHEREAS, various appropriation and revenue accounts must be adjusted in order to accommodate the aforementioned funding, now, therefore, be it

RESOLVED, that the County Administrator is hereby directed to make the following budgetary changes:

Increase Estimated Revenue Account:

A.311.3645.3644.4389.01	Fed Aid, Other Public Safety Homeland Security Grant	\$40,000.00
-------------------------	--	-------------

Increase Appropriation Accounts:

A.311.3645.3644.20207	Homeland Security Equipment	\$18,750.00
A.311.3645.3644.45401	Small Equipment/tools	\$20,135.00
A.311.3645.3644.46103	Other Travel	\$ 615.00
A.311.3645.3644.46101	Meal Reimbursement	\$ 500.00.

Approved by 8 members of the Finance Committee and 7 members of the Public Safety Committee.

Adopted October 22, 2014 by voice vote.

ACT NO. 482-2014 by Ms. Edstrom and Mrs. Stockman

**AUTHORIZING THE CHAIR TO EXECUTE CONTRACT WITH
OLEAN YMCA FOR YMCA MEMBERSHIPS FOR
FAMILIES WITH CHILDREN AT RISK OF PLACEMENT**

Pursuant to 9 NYCRR Sections 771.6 and 771.7,
Public Law 104-193 and Section 450 of the County Law.

WHEREAS, Act 409-2013 authorized a contract with the Olean YMCA, 1011 Wayne Street, Olean, New York 14760, for the provision of YMCA memberships for family activities for at-risk

youth and families in an effort to reduce at-risk factors and out-of-home placement, the term of which expired September 30, 2014, and

WHEREAS, the County Department of Social Services is desirous of continuing the aforementioned services, and

WHEREAS, the Olean YMCA has agreed to continue the provision of the above-described services for an amount not to exceed \$16,000.00 to be paid on a monthly basis for memberships provided during the preceding month, as invoiced, and

WHEREAS, this program is 100% federally funded, now, therefore, be it

RESOLVED, that the Chair of the Legislature be, and hereby is, authorized and directed to execute a contract, on behalf of Cattaraugus County, with the Olean YMCA, for the provision of the above-described services, for a term commencing October 1, 2014 and terminating September 30, 2015, according to the above-described terms, and be it further

RESOLVED, that upon termination of either state or federal funding for this program, then this program shall be automatically abolished, and be it further

RESOLVED, that such contract shall provide that upon the reduction of any such funding, the County, in its sole discretion, may terminate the contract on thirty (30) days written notice, and be it further

RESOLVED, that in the event of any such reduction, the department head involved shall immediately report such occurrence to the Chairman of the Committee to which the department is assigned, who shall add the matter to the agenda of the Committee's next meeting.

Approved by 8 members of the Finance Committee and 6 members of the Human Services Committee.

Adopted October 22, 2014 by voice vote.

ACT NO. 483-2014 by Ms. Edstrom and Mrs. Stockman

**AUTHORIZING THE CHAIR TO EXECUTE CONTRACT WITH
CATTARAUGUS COMMUNITY ACTION, INC. FOR
WIC LICENSED PRACTICAL NURSING SERVICES**

Pursuant to Section 3602 of the Public Health Law and
Section 450 of the County Law.

WHEREAS, Act 321-2013 authorized a contract with the Cattaraugus Community Action, Inc., 25 Jefferson Street, P.O. Box 308, Salamanca, New York 14779, for the provision of licensed practical nursing (LPN) services for the Health Department WIC Program, the term of which expired September 30, 2014, and

WHEREAS, the County Health Department is desirous of continuing the aforementioned services, and

WHEREAS, Cattaraugus Community Action, Inc., has agreed to provide the aforementioned LPN services to Cattaraugus County for an amount not to exceed \$27,115.00, to be paid on a monthly basis as invoiced, and

WHEREAS, sufficient funds are included in the budget to cover the cost of the aforementioned services, now, therefore, be it

RESOLVED, that the Chair of the Legislature be, and hereby is, authorized and directed to execute a contract, on behalf of Cattaraugus County, with Cattaraugus Community Action, Inc., for the provision of the above-described services, for a term commencing October 1, 2014 and terminating September 30, 2015, and be it further

RESOLVED, that upon termination of either state or federal funding for this program, then this program shall be automatically abolished, and be it further

RESOLVED, that such contract shall provide that upon the reduction of any such funding, the County, in its sole discretion, may terminate the contract on thirty (30) days written notice, and be it further

RESOLVED, that in the event of any such reduction, the department head involved shall immediately report such occurrence to the Chairman of the Committee to which the department is assigned, who shall add the matter to the agenda of the Committee's next meeting.

Approved by 8 members of the Finance Committee and 6 members of the Human Services Committee.

Adopted October 22, 2014 by voice vote.

ACT NO. 484-2014 by Mr. Murphy

**AUTHORIZING THE CHAIR TO EXECUTE AMENDED CONTRACT WITH
CHAUTAUQUA COUNTY FOR
SOUTHERN TIER TASK FORCE DRUG ENFORCEMENT PROGRAM**

Pursuant to Section 119-o of the General Municipal Law and
Section 450 of the County Law.

WHEREAS, Acts 105-2013 and 234-2013 authorized contracts with Chautauqua County for the reimbursement for operational expenses related to the Southern Tier Task Force Drug Enforcement Program, including overtime and fringe benefits for personnel, for the period July 1, 2012 through June 30, 2013, and

WHEREAS, Chautauqua County has requested amendments to the aforementioned contracts to extend the terms through December 31, 2014, and also provide for additional reimbursement in the amount of \$37,500.00 to Cattaraugus County, for the aforementioned purposes, and

WHEREAS, the contracts to be extended and/or amended, are known as Agreement 13-06-02B and Agreement 13-06-02C, now, therefore, be it

RESOLVED, that the Chair of the Legislature be, and hereby is, authorized and directed to execute contract amendments, on behalf of Cattaraugus County, with Chautauqua County and the New York State Division of Criminal Justice Services for the provision of the Southern Tier Task Force Drug Enforcement Program, for a term commencing July 1, 2012 and terminating December 31, 2014, according to the above-described terms.

Approved by 8 members of the Finance Committee and 7 members of the Public Safety Committee.

Adopted October 22, 2014 by voice vote.

ACT NO. 485-2014 by Mr. VanRensselaer and Mrs. Labuhn

**AUTHORIZING THE CHAIR TO EXECUTE CONTRACT
WITH SOUTHERN TIER WEST DEVELOPMENT FOUNDATION
FOR WIRELESS BROADBAND PROJECT WITHIN CATTARAUGUS COUNTY AND
ADJUSTING VARIOUS APPROPRIATION AND REVENUE ACCOUNTS
(Department of Economic Development, Planning & Tourism)**

Pursuant to Sections 363, 366 and 450 of the County Law.

WHEREAS, Act 444-2012 authorized the County to participate in the Connect NY Broadband Grant Program as a partner with the Southern Tier West Development Foundation by contributing an amount of \$50,000.00 as a 20% match for the Wireless Broadband Project within Cattaraugus County, and

WHEREAS, the Southern Tier West Development Foundation has received notification that it has been awarded a grant for the aforementioned Wireless Broadband Project, and

WHEREAS, a contract is necessary in order to pay to Southern Tier West Development Foundation the amount of \$50,000.00, and

WHEREAS, Act 643-2013 established Account A.913.0000 - Fund Balance Committed-Economic Development for unexpended Casino Funds, and

WHEREAS, various appropriation and revenue accounts must be adjusted in order to cover the aforementioned \$50,000.00, now, therefore, be it

RESOLVED, that the Chair of the Legislature be, and hereby is, authorized and directed to execute a contract, on behalf of Cattaraugus County, with Southern Tier West Development Foundation, in order to contribute the amount of \$50,000.00 for the Broadband Wireless Program, for a term commencing October 22, 2014 and terminating December 31, 2014, according to the above-described terms, and be it further

RESOLVED, that the County Administrator is hereby directed to appropriate from Fund Balance Committed Economic Development Account A.913.0000 and make the following budgetary changes:

Increase Appropriation Account:

A.298.6420.0000.42048	STW Devel. Foundation Broadband Project	\$50,000.00.
-----------------------	---	--------------

Approved by 8 members of the Finance Committee and 7 members of the Development and Agriculture Committee.

Adopted October 22, 2014 by voice vote.

ACT NO. 486-2014 by Mr. Klancer and Mr. Murphy
and Mrs. Stockman, Mr. VanRensselaer, Mr. Weller, Mr. Koch, Mrs. Labuhn and Mr. Padlo¹

**AUTHORIZING THE CHAIR TO EXECUTE CONTRACT WITH
TOTAL SENIOR CARE, INC. FOR ASSISTANCE WITH RENOVATIONS AT
GOWANDA ADULT SOCIAL DAY PROGRAM SITE AND
ADJUSTING APPROPRIATION AND REVENUE ACCOUNTS
(Department of Economic Development, Planning & Tourism)**

Pursuant to Sections 363, 366 and 450 of the County Law.

WHEREAS, Total Senior Care, Inc., has been awarded a grant in an amount of \$518,133.00 for the development of adult social day programs in the Gowanda and Wellsville areas, and

WHEREAS, the Gowanda social day program site will be located in the Community Place/Academy Place building at 1 School Street, and

WHEREAS, Total Senior Care, Inc. is requesting Cattaraugus County provide \$23,000.00 to assist with some necessary renovation costs, and

WHEREAS, the County is desirous of assisting Total Senior Care, Inc., with the aforementioned renovation project by contributing the amount of \$23,000.00 towards the cost of such renovation project, and

WHEREAS, the aforementioned \$23,000.00 shall be provided through Casino funds, and

WHEREAS, various appropriation and revenue accounts must be adjusted in order to accommodate the aforementioned \$23,000.00, now, therefore, be it

RESOLVED, that the Chair of the Legislature be, and hereby is, authorized and directed to execute a contract, on behalf of Cattaraugus County, with the Total Senior Care, Inc., in order to provide the aforementioned funding, for a term commencing October 22, 2014 and terminating December 31, 2015, according to the above-described terms, and be it further

RESOLVED, that the County Administrator is hereby directed to appropriate from Fund Balance Committed Economic Development Account No. A.913.0000, and make the following budgetary changes:

Increase Appropriation Account:

A.298.6055.0000.42049	Total Senior Care, Inc.	\$23,000.00.
-----------------------	-------------------------	--------------

Approved by 7 members of the Finance Committee and 7 members of the Development and Agriculture Committee.

¹The following Legislators requested their names be listed as additional sponsors: "Mrs. Stockman, Mr. VanRensselaer, Mr. Weller, Mr. Koch, Mrs. Labuhn and Mr. Padlo".

Adopted October 22, 2014 by voice vote.

ACT NO. 487-2014 by Ms. Edstrom and Mrs. Stockman
who ask immediate consideration

APPOINTMENTS TO COMMUNITY SERVICES BOARD

Pursuant to Section 41.11 of the Mental Hygiene Law.

RESOLVED, that the following individual is appointed to the Community Services Board effective October 3, 2014 with a term to expire December 31, 2016:

William F. Mills, M.D.
1732 David Drive
Olean, New York 14760
(due to the resignation of Alan Barlow),

and

RESOLVED, that the following individual is appointed to the Community Services Board effective October 3, 2014 with a term to expire December 31, 2017:

Gail S. Mayeaux
4641 Lower Birch Run Road
Allegany, New York 14706
(due to the resignation of Laura Elliott-Engel).

MS. VICKMAN moved, seconded by Mr. Boser to waive Rule 12. Carried.

Adopted October 22, 2014 by voice vote.

ACT NO. 488-2014 by Mr. Marsh
and Mr. Sprague¹
who ask immediate consideration

**AUTHORIZING THE CHAIR TO EXECUTE CONTRACTS WITH
CORNELL COOPERATIVE EXTENSION - CATTARAUGUS COUNTY AND AN
INDEPENDENT AUDITOR FOR ASSISTANCE WITH FISCAL AUDIT
AND TRANSFER OF FUNDS
(Contingent Fund – Audit Services Contracted)**

Pursuant to Sections 363, 365 and 450 of the County Law.

WHEREAS, Cattaraugus County is requiring Cornell Cooperative Extension to hire an independent auditor for an audit of fiscal year 2013 and three quarters of fiscal year 2014, and

WHEREAS, Cornell Cooperative Extension shall obtain quotes from several auditors and forward them to the County for review and approval, and

WHEREAS, upon such review and approval, the County shall advise Cornell which auditor it shall use for the audit, and

WHEREAS, the auditor shall audit Cornell's records for fiscal year 2013 and three quarters of fiscal year 2014, and

WHEREAS, upon the completion of such audit, the auditor shall present its findings to the Cattaraugus County Legislature, and

WHEREAS, the County shall pay to such auditor an amount not to exceed \$7,500.00 towards the cost of the audit, and

WHEREAS, a transfer of funds is necessary in order to cover the cost of the aforementioned auditor services, now, therefore, be it

RESOLVED, that the Chair of the Legislature be, and hereby is, authorized and directed to execute contracts, on behalf of Cattaraugus County, with Cornell Cooperative Extension-Cattaraugus County and an independent auditor, for the provision of the above-described auditing services, for a term commencing October 22, 2014 and terminating December 31, 2014, according to the above-described terms, and be it further

RESOLVED, that the County Administrator is hereby directed to make the following budgetary changes:

Decrease Appropriation Account:

A.901.1990.0000.40601	Contingent Fund	\$7,500.00
-----------------------	-----------------	------------

Increase Appropriation Account:

A.901.1910.0000.41208	Audit Services Contracted	\$7,500.00.
-----------------------	---------------------------	-------------

MR. TEACHMAN moved, seconded by Mrs. Labuhn to waive Rule 12. Carried.

¹The following Legislator requested his name be listed as an additional sponsor: "Mr. Sprague".

Adopted October 22, 2014 by voice vote. Ms. Edstrom and Mrs. Stockman voting No.

ACT NO. 489-2014 by Mr. Edwards
who asks immediate consideration

**AUTHORIZING THE CHAIR TO EXECUTE A CONTRACT WITH
AIG TO PROVIDE CYBER CRIME INSURANCE COVERAGE TO THE COUNTY**

Pursuant to Section 92-a of the General Municipal Law and
Section 450 of the County Law.

WHEREAS, Act 603-2012 authorized a contract with Marsh USA, Inc., for the provision of services required to serve as Insurance Broker of Record for the County's Property, Boiler & Machinery, Excess Public Entity Liability, Commercial Crime, Excess Workers' Compensation & Employer's Liability, and Pines Fidelity Bond Insurance coverage, and

WHEREAS, Cattaraugus County is desirous of obtaining Cyber Crime Insurance coverage to mitigate potential risks to the County's computer systems, networks and information technology services, and

WHEREAS, Marsh USA, Inc., has solicited information from various vendors who are able to provide Cyber Crime Insurance coverage, and

WHEREAS, Marsh USA, Inc., has made a recommendation based on a risk analysis of the County's technical needs for the anticipated levels of exposure to potential threats, and

WHEREAS, the County Attorney, Information Services Director, County Administrator, and Human Resources Director have reviewed the various coverages available and have recommended an appropriate level of coverage, and

WHEREAS, American International Group, Inc. (AIG) has agreed to provide Cyber Crime Insurance, through the Illinois National Insurance Company, for a premium amount of \$33,876.00, and

WHEREAS, sufficient funds are included in the budget to cover the cost of the aforementioned insurance coverage, now, therefore, be it

RESOLVED, that the Chair of the Legislature be, and hereby is, authorized and directed to execute a contract, on behalf of Cattaraugus County, with AIG for the provision of the above-described Cyber Crime Insurance program, for a term commencing October 21, 2014 and terminating October 21, 2015, according to the above-described terms.

MS. EDSTROM moved, seconded by Mr. Lamberson to waive Rule 12. Carried.

Adopted October 22, 2014 by voice vote.

MS. EDSTROM moved, seconded by Mr. Sprague to adjourn until November 12, 2014 at 3:00 p.m. Carried.

Meeting adjourned at 3:42 p.m.

Ann M. Giglio
Journal Clerk