ERIE COUNTY WATER AUTHORITY
INTEROFFICE MEMORANDUM

February 13, 2019

To: Commissioners Schad, Carney and Jones

From: Robert J. Lichtenthal, Jr., Deputy Director

Subject: Update on the Corrective Action Plan for OSC Technology Audit 2016-2017

The Office of the New York State Comptroller (OSC) conducted an audit of the Authority to determine whether Authority officials adequately safeguarded and protected information technology (IT) assets, used in its business environment, against unauthorized use, access and loss. The audit period was from January 1, 2016 to October 6, 2017 with draft reports received in March, 2018 and a final report received in April, 2018. Attached is a copy of the final report issued after an exit conference with Authority staff and the Board Treasurer.

The Authority was required to file a plan of corrective action within 90 days from the issuance of the report. The report was issued May 4, 2018. At the Governance Committee meeting on August 2, 2018 a plan of corrective action was approved and filed with the Office of State Comptroller. A copy is attached.

At this time I wanted to provide the Governance Committee an update on the implementation of the corrective plan.

NYS OSC Finding #1

Authority officials did not develop procedures for managing system and network access

NYS OCS Recommendation:

Authority Officials Should:

Develop and implement written procedures for managing System and network access that include periodically reviewing user access and disabling or deleting user accounts when access is no longer needed.

Attached is a written procedure that the IT Department is following effective January 1, 2019. This written procedure follows what the IT Department has been generally doing in the past but which had not been formalized in writing. This has been corrected.

NYS OCS Finding #2

Internet usage was not routinely monitored

NYS OSC Recommendations:

The Board should:

Work with Authority officials to review and update the computer use policy and then ensure the IT Manager includes the updated policy when providing cyber security training to all employees.

The NYS OSC recommendations included three issues to be addressed:

1. Update the Computer Use Policy
2. Providing the updated policy to all employees during cyber security training
3. The finding that internet usage was not routinely monitored

Attached to this memo is a draft revised copy of ECWA Policy No. 89.0, Computer, Internet, Electronic Commerce and E-Mail Policy. This draft revised policy adds provisions for cyber security training and recommends other changes that reflect the current operating environment of the Authority. The section on cyber security training was developed in consultation with the Director of Human Resources and the Acting Director of IT.

The portion of this recommendation for which a total solution has not been identified is the concept of routine monitoring of internet usage. Based upon the sheer number of internet enabled devices that the Authority has deployed as a part of the ECWA Advance project and the number of employees that now have internet access to do their job, the concept of being able to monitor the internet usage log for all instances of potential improper usage is daunting. As of now a time and cost effective method has not been identified and staff will continue to attack this matter.

NYS OSC Finding #3

The Authority does not provide adequate cyber security training to employees.

NYS OSC Recommendations:

Ensure that cyber security training is provided periodically to all employees to address current and emerging risks.

I conferred with the Authority's Claim Representative/Risk Manager Anthony Alessi regarding cyber security training resources that the Authority's provider of Cyber Liability insurance might be able to provide or recommend to the Authority. The carrier, Chubb/Ace American Insurance Co., does provide a training resource which I myself took advantage of. While I will not hold myself out as an expert in this field, I did find this training helpful and I believe that as a first step on a never ending journey of cyber security awareness for our employees, this training would be a good first step for all of the Authority's staff. This training would also allow additional time for the Authority to identify and develop additional training resources to be utilized for ongoing training.

When final action on proposed revisions to Policy No. 89 are approved by the Commissioners, the IT Department and Human Resources will work to implement the training immediately. In addition, an annual review of Policy No. 89 will be incorporated into the Authority's Annual Employee Performance Review process.

ECWA System and Network Access Procedures

January 1, 2019

1. **<u>Request to create a system user and grant/modify systems and network access</u>** – Supervisor of employee to complete the Information Technology Service Request Form or email the IT Manager with the requesting Department Head cc'd. With IT Manager approval, the IT Security Officer will proceed to create a profile and grant/modify access to the requested systems:
    a. Create user profile using individuals initials (First, Middle, Last) XXX
        i. Power System- Verify the initials aren't currently used or were used by a former employee using menu options 880/150 - System User ID Maintenance. If they were, add a numeral after the 3 initials, increment sequentially if necessary. XXX#
        ii. Power System – Create profile using CRTUSRPRF command.
        iii. Active Directory – Add user profile created on the Power System to "Users" group. Populate First and Last name fields. If the user is a consultant, add Company Name to Display Name field.
        iv. Active Directory – add user to the QSSO Global Security Policy group for password complexity and password expiration management.
        v. Active Directory – Dial-In tab under Network Access Permission select:
            1. Allow access - VPN and WiFi access
            2. Deny access – no VPN or WiFi access
            3. Control access through NPS Network Policy – WiFi only
    b. Power System menu's (Billing, Payroll, Purchasing …. Inquiry/Maintenance)
        i. Power System- Menu 880/130 Security Maintenance by User/Menu.
    c. Cityworks Access
        i. Cityworks – Menus Designer, Employees.
        ii. Active Directory - Add user to proper access group.
    d. Network Folders
        i. Power System – Update folder Authorization List. (CHGAUTL) Folder access controlled by authorization lists on Power System.
    e. Email Account
        i. Exchange Server – Create mailbox
    f. Phone Extension
        i. AVAYA Site Administration – add extension
    g. Voicemail
        i. Web Browse to Phone Switch - Menu Messaging - add Voicemail box
    h. Internet Access
        i. Service Center Firewall and Ellicott Square Firewall – Add IP address to Internet_Access_Web-Host group. Internet access granted by IP address.
    i. Device Access – PC/Laptop/Tablet/Cell Phone -Device Ethernet/Wi-Fi MAC Address needed for MAC authentication with RADIUS Server.
        i. Active Directory – add MAC address to AD MAC_AUTH Group. Control what devices can access the ECWA network.

ii. Power System – Menu 880/920 or 930 Login Restrictions by Computer or User. Control who can sign onto a particular PC.

iii. Information Technology group configures Ethernet and Wi-Fi on all devices that connect to ECWA network. Users do not have local admin rights on the devices.

j. SCADA Access – Request from Chemist/Chief WTPO or Production Engineer

i. Active Directory - Add user to proper access group.

k. Door Access – Request from Human Resources

i. B.A.S.I.S. System – Create badge, grant access to requested doors.

2. **Revoke User Systems and Network Access –** Human Resources notifies the IT Manager that an individual in no longer employed by the Authority. The IT Security Officer immediately:

a. Disables User Profile

i. Active Directory – Disables user profile by right clicking and selecting “disable”. The individual immediately loses the ability to log into Domain connected PCs, Laptops and Servers including SCADA. They are also denied access to ECWA email.

ii. Power System – Disable the user profile by changing the status field to “*disabled” using WRKUSRPRF. The individual immediately loses access to Network Folders and Power System menus.

b. Disable Door Access

i. B.A.S.I.S. System – Change Badge Status from “Active” to “Returned”. The badge will no longer unlock ECWA doors.

c. Disable Device Access

i. Active Directory - Delete entry in MAC-AUTH group.

3. **Removal of user profile, email and voicemail**

i. Exchange Server - Backup users email to a .pst and copy to network drive for backup and archival purposes. Delete mail box.

ii. Active Directory - Delete user profile from Users group.

iii. Power System – After a monthly system backup is performed, the Security Officer runs a procedure to backup then delete Power System program access, backup and delete file authorizations, change ownership of user’s IFS files, and finally deletes the user profile.

iv. Voicemail – After verifying no new voicemails have been received, delete the voicemail box.

4. **Monthly Review of Active Directory “USERS” and “MAC_AUTH” groups**

i. Visually review current list of users and MAC addresses for people that have recently left the employ of the Authority.

ii. Run Power Shell commands to list users or MAC addresses that haven’t been logged into in the past XX days.

ECWA Internet Usage Monitoring Procedures

January 1, 2019

1. **Quarterly Random Review of Internet Usage**

   i. Review list of employees with internet access over the previous three months
   ii. Randomly choose 5 Authority departments
   iii. Randomly choose 2 employees from each department
   iv. Visually review internet browsing history log of the selected employees and noting potential sites visited which violate usage guidelines
   v. Prepare a report and forward to Human Resources Department
   vi. Human Resources Department will forward Department specific results to the 5 Departments surveyed for the quarter
   vii. Department and Unit Heads (and Human Resources if necessary) will review any inappropriate activity with employees in accordance with all Authority disciplinary procedures

ERIE COUNTY WATER AUTHORITY
HR Policies/Procedures

Re:	**COMPUTER, INTERNET, ELECTRONIC COMMERCE AND E-MAIL POLICY**	**Policy No.:**	**89.0**
Application:	**All Employees**	**Adopted:**	**04/29/99**
		Amended:	**12/04/03** **12/02/10** **01/26/12**

ERIE COUNTY WATER AUTHORITY
COMPUTER, INTERNET, ELECTRONIC COMMERCE, E-MAIL, SOCIAL NETWORKING AND WIRELESS COMMUNICATION DEVICE POLICY

Introduction:

The Erie County Water Authority ("Authority") provides computer and Internet access for business transactions, electronic business data transfer, electronic commerce, electronic mail, web transaction account services and procurement.

Internet usage, electronic commerce and e-mail refers to the electronic transfer of information typically in the form of electronic messages, memoranda and attached documents from a sending party to one or more receiving parties. The term e-mail can refer to an electronic mail *service* or an electronic mail *message*. Well-designed and properly managed electronic data transmission systems expedite business communications, reduce paperwork and automate routine office tasks thereby increasing productivity and reducing costs. These opportunities are, however, at risk if electronic data systems are not used and managed effectively.

This Policy advises staff and management of their responsibilities and provides guidance in using and managing information in the Authority's computer system or communicated by Authority e-mail, electronic commerce or electronic data transfer systems.

Internet and e-mail access is a service provided by the Authority that enables participating departments, units and individual employees to send and receive messages and utilize related utilities in the performance of their job duties. It is for Authority business use only and is to be used with discretion. To request e-mail services over the Internet a Data Processing Service Request Form must be approved by your Department Head and submitted to the Manager of Data Processing.

The Authority may store electronic communications for a period of time after the communication is created. From time to time, copies of communications may be deleted.

The Authority's policies prohibiting harassment apply to the use of the Authority's email, ~~,~~ communication and computer systems. No one may use any email, communication or computer system in a manner that may be construed by others as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs or any other characteristic protected by federal, state or local law.

Since the Authority's email, communication and computer systems are intended for business use, the mail and these systems may not be used to solicit for religious or political causes or outside organizations.

Unauthorized duplication of copyrighted computer software and computer files and documents violates the law and is strictly prohibited.

No Employee may access, or attempt to obtain access to, another Employee's email or computer systems without appropriate authorization.

Violators of this policy may be subject to disciplinary action, up to and including discharge.

I. CYBERSECURITY AWARENESS AND TRAINING

Formatted: Font: Bold

Formatted: Indent: Left: 0", Hanging: 0.25", Numbered + Level: 1 + Numbering Style: I, II, III, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.75", Tab stops: 0.25", Left + Not at 0.62"

Formatted: Font: Bold

Formatted: Line spacing: single, Tab stops: 0.5", Left + 0.56", Left

Recognizing the critical nature of the Authority's operations with respect to Public Health & Safety and the negative impact any attack on or breach of the Authority's information technology systems would have to those operations, all employees must at all times take all necessary precautions to protect the Authority's information technology assets.

All new employees will be provided Cyber Security Awareness Training during their initial orientation. All employees will be subject to updated training on an annual basis. The training subject matter and delivery mechanism will be developed by the IT Department. A record of an employee's successful completion of every training session will be provided by the IT Department to the Human Resources Department for inclusion in the employee training record file.

As an additional layer of attention to cyber security, all supervisors will review the most current Computer, Internet, Electronic Commerce and E-Mail Policy with employees during their annual performance appraisal.

~~I~~ II. ***Guidelines For Use of Authority's E-Mail System:***

E-mail (electronic mail) is used in the normal course of Erie County Water Authority business for general business communication as well as sharing of files. While immediate and sometimes informal, electronic mail may, under certain circumstances, serve as a record of a decision or other official action. It is important to recognize that an e-mail message, created or received by Authority personnel in connection with official business is a record that is subject to access, privacy and records management laws and regulations.

E-mail should be used for business purposes only and should not be of a confidential or personal nature. E-mail messages sent or received on the Authority's computer and communication systems may be accessed and monitored in the normal course of business by system administrators, supervisors, and support staff; may be releasable to the public under the Freedom of Information Law (FOIL); may require special measures for privacy protection to comply with the Personal Privacy Protection Law (PPPL); and may be subject to discovery proceedings in legal actions. **Users have no expectation of privacy in regard to any information stored in the Authority's computer, communication or e-mail systems.**

E-mail is the property of the Erie County Water Authority. Stored e-mail messages are not personal and private. Technical staff will not routinely monitor e-mail, but will monitor or copy stored emails if and when appropriate for business reasons.

The Manager of Data Processing, the Secretary to the Authority, or an individual designated by the Authority may access voice-mail, e-mail, wireless communication devices, and any other accounts where it is deemed appropriate,

Employees are responsible for monitoring their own address and related e-mail. If an extended absence or similar situation occurs, it is the responsibility of each employee to temporarily redirect e-mail messages or allow a third person to receive that individual's e-mail.

Basic Format:

Employees sending e-mail will include their name and title at the end of the message. If the message concerns a project, the project number (or equivalent) shall be included on the subject line. For messages that transmit a draft attachment, the message shall reference the document's project number (or equivalent) and the word draft in the subject field.

Records Management:

E-mail messages and electronic data transfers are records when they are created or received by the Authority in the normal course of official business and should be preserved, or are appropriate for preservation, as evidence of the organization's actions, official policies, decisions, procedures, transactions, functions, operations or other activities of the Authority or because of the informational content. E-mail meeting these criteria are subject to records management requirements.

Examples of messages sent by e-mail that typically are records include:

- ! policies and directives
- ! correspondence or memoranda related to official business
- ! work schedules and assignments
- ! agendas and minutes of meetings
- ! drafts of documents that are circulated for comment or approval
- ! any document that initiates, authorizes, or completes a business transaction
- ! all purchasing and procurement communications
- ! final reports or recommendations.

Examples of messages that typically <u>do not</u> constitute records are:

- ! personal messages and announcements
- ! copies of extracts of documents distributed for convenience or reference
- ! phone message slips
- ! announcements of social events.

E-mail is a transient record. Messages which are used to support business purposes should, therefore, be stored in one or more of the following ways:

1) Moved to a designated, named electronic folder (i.e. AI≅ Drive, main folder ($proj), sub-folder (ECWA), sub-folder (P199900032)
2) Saved as a file and placed in an appropriate directory
3) Printed and then given to Records Management personnel for filing in the proper folder.

Records needed to support program functions should be retained, managed, and accessible in existing filing systems outside the e-mail system. System capacity requires periodic deletion of old messages and user queued items. Users are encouraged to delete messages and queued items daily. This includes messages stored in the Ain basket≅, the Aout basket≅ and Awastebasket≅. Before deleting any e-mail message, however, determine whether it meets the legal definition of a record. If the e-mail message is a record, print it or transfer it to other files before deleting from the computer. Be certain the printed message contains time essential transmission and any requested receipt data. If not, print the data or annotate the printed copy. File the printed message and essential transmission and receipt data with related files of the office.

Records communicated using e-mail need to be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Disposition of these records will be in accordance with the Authority=s Records Retention Schedules. Records may not be destroyed without a Records Disposition Authorization approved by the State Archives and Records Administration.

The system administrator will purge from the Apost office≅ e-mail messages stored on the AS/400 on a weekly basis.

<u>Security:</u>

The Authority reserves the right to monitor the system for maintenance, repair, help functions, troubleshooting, suspected abuses of e-mail privileges, and other legitimate business reasons. While the communications are protected by passwords, they are not secure and, in appropriate circumstances, there may be administrative access to these records. Keep this in mind when choosing topics for e-mail communications.

All access to an employee's e-mail will be denied upon termination of his/her employment and the e-mail account will be canceled. The systems administrator will oversee the distribution of existing e-mail in a closed account to appropriate electronic or paper folders.

Users must take all reasonable precautions, including changing passwords, to prevent use of your account by unauthorized individuals. Passwords, and the ability to frequently change passwords, can facilitate e-mail security. Unchanged passwords will expire after 60 days and must be re-entered. Forgotten passwords can be reset to a new temporary password by calling the Help Desk at Ext. 8211(685-8211).

Administrative access to an employee's individual computer will be controlled by the Security Officer. The Authority will require that all Authority personal computers be protected with passwords that prevent their use by unauthorized users. However, employees should take notice that the use of a password or pass code by an employee does **NOT** ensure privacy, and any record may be accessed by an individual designated by the Authority.

Personal Use:

Rules for personal use of e-mail or other electronic communications are the same as for personal use of the telephone. Only incidental personal communications by fax or e-mail to family or friends sent on personal time (break, lunch, etc.) are acceptable.

Prohibited Uses of E-Mail or Computers:

The following uses of Authority computer facilities are prohibited:

- ~~!~~ access to or use of obscene or potentially harassing graphics, documents or web sites
- ~~!~~ ~~documents or e-mail relating to personnel, time and attendance or union business~~ documents or e-mail strictly related to internal Union-related business. This does not restrict communications between Union officials and Authority management staff
- ~~!~~ personal business (a profession, banking, purchasing, stock market transactions, etc.)
- ~~!~~ consumption of Authority resources (e.g. long-distance charges or extended local phone connections)
- ~~!~~ personal charges to the Authority through the use of Authority e-mail capabilities

Formatted: Bulleted + Level: 1 + Aligned at: 0.8" + Indent at: 1.05"

- ~~!~~ unauthorized access to e-mail accounts
- ~~!~~ use for private or personal business, other than incidental use
- ~~!~~ unauthorized or unnecessary connections to outside networks
- ~~!~~ illegal, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interest of the Authority.

~~II~~ III. ***Guidelines For Use of Authority’s Access to the Internet:***

A. General Guidelines

This policy sets forth guidelines about the personal use of the ~~the~~ Authority’s Internet access. Currently, access to the Internet is provided to employees when there is a necessity and the access has been specifically approved.

The Authority has provided access to the Internet for authorized users to support the business purposes of the Authority. No use of the Internet should conflict with the primary business purpose of the Authority or with applicable laws and regulations. As a condition of continued employment, each user is personally responsible to ensure that these guidelines are followed.

The Authority may monitor usage of the Internet by employees, including reviewing a list of sites accessed by an individual. No individual can have any expectation of privacy with respect to his or her usage of the Internet on the Authority’s system. In addition, the Authority may restrict access to certain sites that it deems are not necessary for business purposes.

Employees are prohibited from encrypting files on their computers or taking any steps that block access to files, other than the use of the Authority’s passwords or approved encryption programs. Employees must not change their logon codes. Employees may never change the default settings in the devices “internet options” (i.e. how long history and temporary files are stored, internets security settings, etc…). The deletion of the devices history, temporary files or internet downloads is also prohibited.

The Internet provides access to many sites that charge a subscription or usage fee to access and use the information on the site. If costs are appropriately incurred on behalf of the Authority, the user may submit the charges for reimbursement on expense reports, subject to customary review. All items that are charged to the Authority are subject to the same approval process as other business-related expenses. Requests for approval should be submitted accordingly.

The Authority's connection to the Internet may not be used for any of the following activities:

1. The Internet must not be used to access, create, transmit, print or download material that is derogatory, defamatory, obscene, or offensive, such as slurs, epithets, or anything that may be construed as harassment or

disparagement based on race, color, national origin, sex, sexual orientation, age, disability, or religious or political beliefs.

2. The Internet must not be used to access, send, receive, or solicit sexually oriented messages or images.

3. Downloading or disseminating of copyrighted material that is available on the Internet is an infringement of copyright law. Permission to copy the material must be obtained from the publisher. For assistance with copyrighted material, contact the ~~Data Processing Department~~Information Technology Department.

4. The downloading or posting of any copyrighted material from any source to the Authority's network is an infringement of copyright law. Permission to copy the material must be obtained from the publisher.

5. Without prior approval of the ~~Data Processing Department~~Information Technology Department, software should not be downloaded from the Internet as the download could introduce a computer virus onto the Authority's network. In addition, copyright laws may cover the software so the downloading could be an infringement of copyright law.

6. Employees should safeguard against using the Internet to transmit personal comments or statements through e-mail or to post information to newsgroups or Usenet that may be mistaken as the position of the Authority.

7. Employees shall guard against the disclosure of confidential information through the use of Internet e-mail, news groups or Usenet.

8. The Internet shall not be used to send or participate in chat rooms, chain letters, pyramid schemes or other illegal schemes.

9. The Internet should not be used to solicit or proselytize others for commercial purposes, causes, outside organizations, chain messages or other non-job-related purposes.

In the event that an employee unintentionally or accidentally performs one of these prohibited actions, the employee must report the action immediately to the Manager of Data Processing or Secretary to the Authority.

B. Guidelines governing Blogging and On-Line Social Networking

The Authority respects the right of any Employee (on personal time, with personal equipment) to maintain a blog and to utilize social networking sites. However, to protect the Authority's interests and ensure Employees focus on their job duties, Employees must adhere to the following rules and conditions. It is the policy of the Authority that its employees use computers, computer applications, computer programs, Internet resources and network/Internet communications in a responsible, professional, ethical, and lawful manner.

The term “social networking“ includes social network sites that use Internet services to allow individuals to construct a public or semi-public profile within that system, define a list of other users with whom they share some connection, and view and access their list of connections and those made by others within that system. Examples of the types of Internet based social networking sites include: blogs, networking sites, photo sharing, video sharing, microblogging, podcasts, as well as comments posted on the sites. Some social networking sites include Facebook, LinkedIn, Twitter, MySpace, and Youtube. The absence of or lack of explicit reference to a specific site or type of site does not limit the extent of the application of this policy.

1. Employees may not post on a blog or utilize social networking sites during work time or with Authority equipment or property.

2. All rules regarding confidential information apply in full to blogs and social networking sites. Any information that cannot be disclosed through a conversation, a note or an e-mail also cannot be disclosed in a blog or a social networking site.

3. If Employees mention the Authority in a blog or social networking site and also express a political opinion or an opinion regarding the Authority’s actions, the poster/user must specifically note that the opinion expressed is his/her personal opinion and not the Authority’s position. This is necessary to preserve the Authority’s good will in the marketplace. If the employee identifies their employment with the Authority they take on the responsibility for representing the Authority in a professional manner from that period forward while still employed by the Authority.

4. Any conduct which under the law is impermissible if expressed in any other form or forum is impermissible if expressed through a blog or social networking site.

5. Some blogs or social networking sites require that users agree to abide by a terms of service (TOS) document. Authority employees are responsible for reading, knowing, and complying with the TOS of the sites they use.

Further, the Authority encourages all Employees to contemplate the speed and manner in which information posted on a blog or social networking site can be relayed and often misunderstood by readers. Thus, subject to the limited restrictions above, while an Employee’s free time is generally not subject to any restrictions by the Authority, the Authority urges all Employees to not post information regarding the Authority or their jobs which could lead to morale issues in the workplace or which could detrimentally affect the Authority’s business.

~~III~~ IV. ***Wireless Communication Device Usage:***

It is the Policy of the Authority to provide Wireless Communication Devices to those individuals who are required to respond in the business operation of their normal assignment.

A Wireless Communication Device is defined as a cellular telephone, smart phone web enabled handset, ~~or a~~ laptop computer or tablet.

It is the Policy of the Authority that these devices are to be used for business purposes only and that any personal calls are minimal. A charge of $.20 per minute ~~shall~~ may be reimbursed to the Erie County Water Authority for any personal usage. Downloads of content or applications must be for business purposes only and should have prior approval by the Department Head and Director of Administration. In the case of downloads of content or applications to laptop computers and tablets, prior approval by the Department Head and the Secretary to the Authority is required. Unauthorized downloads of content and applications are prohibited.

It is the policy that any and all laws restricting the use of such devices while driving a motorized vehicle be enforced. The Authority prohibits driving and using such devices without the usage of a proper hands-free adapter.

Procedures:

The Director of Administration shall administer the distribution and control of wireless communication devices (not including laptop computers or tablets). The distribution and control of laptop computers and tablets shall be administered by the ~~Secretary to the Authority~~Information Technology Department. Wireless communication device usage invoices will be made available to the Department Head and then to the user for review.

The Comptroller, on behalf of the Authority, shall receive all personal use funds.

~~I~~V. ***ECWA On-Line Request For Change:***

The Erie County Water Authority On-Line Request for Change form should be used to post and update new data on our web site. All requests must be accurate and forthright and require proper levels of approval before they are sent to our web site developer for posting. All requests will be filed in Central Files at Ellicott Square.