Agenda and Topics

Business Continuity Planning
- Terms: Business Continuity, Disaster Recovery
- MCLS Business Continuity Focus

MCLS IT Vulnerability
- Web & Email vulnerabilities
- Areas of Responsibility

IT Related Policies
- MCLS Breach Notification, MCLS Email Use
- Discussion on other policies, procedures
A business continuity plan is a plan to help ensure key business processes can continue during a time of disruption or disaster.

Disruptions might include a fire, flood or instance where operations are not able to occur under normal conditions. They may be limited to your location.

Disasters (natural or man-made) typically have regional implications beyond your operations.
Disaster recovery is the ability to restore data and applications that run your operations if your data center, servers, or other IT infrastructure get damaged or destroyed.

It is a subset of Business Continuity.
Elements of successful business continuity plans:

- Consider location/facility, staffing, equipment
- Consider which operations need to continue during a disaster
- Combine hardware and software technology solutions for “fail over” or secondary applications
- Consider process(es) for data recovery
MCLS Business Continuity Framework

- ILS
- Storage/Data
- Email/Internal Communications
- Network/Internet Access
MCLS Business Continuity: Reducing Risk

MCLS Operational Priority Actions 2013-18

- **Building support:** Rundel fire suppression system 2013
- **Email:** Office 365 migrated to cloud-based email in 2015
- **System data/storage:** Uninterrupted Power Supply 2016
- **MCLS Websites:** Hosted solution 2017
- **Integrated Library System:** Hosted solution 2017
- **System data/storage:** Offsite backup solution 2018
Future MCLS Operational Priority Actions

- **Email**: Vulnerability assessment (spam testing, etc.)
- **System data/storage**: Evaluation of full hosting (AWS or Azure)
- **Data Breach Notification**: Draft Policy for MCLS Approval
- **Documentation**: Completion of Business Continuity Plan

MCLS administration considers intentional network disruption (hack, malware, etc.) a higher likelihood than facility or natural disaster.
IT Vulnerability for MCLS
Web Vulnerabilities

- Bots
- DDoS
- Cross-site scripting
- Malware

See vulnerability glossary

Vendors addressing vulnerability

- Zayo (ILS host)
- MCLS
- Blue Tower (web host)
Email Vulnerabilities

- Malware
- Phishing
- Unintentional data sharing by staff
- Intentional act(s) by staff or former staff

Who needs to address vulnerability:

- Microsoft (O365)
- MCLS
- Member Libraries

See vulnerability glossary
## Areas of Responsibility

<table>
<thead>
<tr>
<th>System</th>
<th>Member Library</th>
<th>Shared</th>
</tr>
</thead>
</table>
| • Email system  
• ILS  
• Libraryweb.org  
• 3rd party payment processing  
• System data/storage  
• Shared software solutions & applications | • Hardware (computer use)  
• Internal data/storage  
• Internal network  
• Staff vulnerability (authorizations, assessments) | • Shared/Wide area network  
• Email account maintenance  
• Staff technology use training |
IT Related Policies
NYS Breach Notification Law Changes


It now provides that persons or businesses conducting business in New York must disclose any breaches of computerized data which includes private information by notifying the offices of the New York Attorney General; the NYS Division of State Police; and the Department of State's Division of Consumer Protection.
MCLS Breach Notification Policy

**MCLS policy purpose is to...**

* provide guidance to enable quick and efficient recovery from security incidents
* identify steps necessary to handle an incident, minimize disruption to services and address loss/theft of information.
* describe: 1) who to notify upon discovery of an incident; 2) procedure(s) for handling and recovering from an incident based on incident type; 3) reporting format; and 4) evidence retention procedure.
Email Use Policy

Reminder that policy is signed by all staff as part of email registration.

Policy & guidelines available on ePortal

MCLS Governance:

MCLS Overview:

Policies & Procedures

Monroe County Library System Email Use Policy

The Monroe County Library System’s (MCLS) electronic communications, including Internet access and email, are made available to all member library employees to carry out the business of the MCLS. All MCLS email communication and information transmitted, received and/or stored are the property of the MCLS.

Correspondences sent using an MCLS email account are subject to the Freedom of Information Law and are part of the public record. The content and the tone used in internal or external emails can be interpreted as representing the organization as a whole; it is important to understand this context when composing and sending emails.

MCLS email should not be used for distribution of content that is in violation of a copyright, obscene or harassing material, or material which promotes religious, political or other personal positions or agendas not associated with the MCLS or with member libraries. MCLS e-mail accounts should not be used as personal e-mail addresses or for personal correspondence.

The MCLS may access its electronic communications and obtain the text of communications of employees within the MCLS. MCLS administration may request such access in order to maintain the email system, in case of emergency, to comply with a valid legal and regulatory order for information, or to ensure continuity of MCLS operations during an employee’s absence.

Employees of MCLS member libraries found to have violated this policy may be subject to member library director notification by MCLS administration. Member libraries are responsible for employee notification of policy violation, remediation of violation and any disciplinary action. MCLS reserves the right to temporarily suspend email access if the account use is in violation of MCLS policy or poses a risk to the MCLS network.

I have read and accept through my applicant signature the MCLS Email Use Policy as stated above.

Applicant’s Name (please print): ____________________________

Library: __________________ Division/Department (Central Only): ______________________

Monroe County Library System Email Use Policy

I have read and accept through my applicant signature the MCLS Email Use Policy as stated above.

Applicant’s Signature: ____________________________ Date: ______________________

Library Director/Department Head Signature: ____________________________

Revised 7/15/2015
Integration of Planning

Discussion: Role of MCLS as supportive organization for member planning, policy development
Actions for Director’s Council

**Endorse MCLS Breach Notification Policy**
- Receive draft for February 2019 MCLS Director’s Council
- Submit to MCLS Board of Trustees March 2019

**Review internal policies and procedures**
- Staff computer use, application authorization/access, account management, etc.
- Business continuity / Disaster recovery (with town/City)

**Training feedback**
- Identify areas of priority technology training
- Process to share results of email vulnerability assessments