CONSIDERATIONS FOR DIGITAL & ONLINE SECURITY AT JEWISH INSTITUTIONS

Email

- It is recommended that Institution officers, employees and key members should have email accounts and email addresses that are institution specific and not connected to private, home or business email accounts.

- For the sake of consistency and security Institution specific email accounts should be the only email addresses used for institution business, community activity and communication internally and externally.

- It is good practice that Institution email addresses should not reflect a person's name, location or any other online identity or presence (Facebook, LinkedIn, etc)

- It is helpful to discuss and initiate a codified policy for the use of Institutional emails, who is entitled to have one and who is in charge of managing their distribution.

- When an email announcement is sent from an institution to a large list of recipients, the email addresses for the intended recipients should be place in the "bcc" (Blind Carbon Copy) area of the addressee section of the email. This will prevent member names from being revealed if the email is forwarded to a third party by a member.

Threatening or Abusive Email

- It is highly recommended that individuals never respond to threatening, abusive, hateful or inflammatory email from anyone you do not know personally.

- Threatening or abusive emails that may need investigation should not be moved from the email box where they are received. They may be forwarded or copy & pasted, but the new copy will not retain information coded into the delivery information of the original message. It is usually best to wait for instructions before transferring or transmitting such emails as the wrong action could remove hidden information that is critical.

- Contact the local police to report the incident, providing examples of what the emails say.

- Contact your email services provider and report the abusive email.

 605 Third Avenue, New York, NY 10158 www.adl.org contactus@adl.org

- Contact the email provider that was used to send the abusive message.

Website

- An Institutional should always make the effort to have their Website hosted with a professional Web hosting company and avoid having the Website reside on an Institution or member's home computer

- Institutions should meet or conference with their Web hosting service and ask about such things as active back-up of Website, what security measures do the hosting company use to prevent Denial of Service (DoS) attacks and unauthorized Website access. Also ask if they have a disaster recovery procedure that includes someone available as a 24/7 point of contact for emergencies.

- As with institutional email addresses, an effort should be made to limit and control the number of people Website administrator or Webmaster permissions and policy for password assignment and a schedule for changing passwords.

Computer Systems

- It is in the best interest of any computer owner to be aware of who has access to their computer, the permissions granted to each account, who has system administrator authorization and who assigns passwords.

- It is now considered a good practice to segregate general office and book keeping/member information to the greatest degree possible.

- If a computer system is connected to the Internet, an institution should consider using a primary carrier (Comcast, TimeWarner, Verizon, etc.) for Internet service. Companies who re-sell other company's services should be avoided where possible.

- It is always prudent to have active and up-to-date firewall, anti-virus and threat detection software.

- Although not all Websites or personal use of an Institution's computers pose a problem, a basic "no personal use" policy is reasonable.

- As a general rule users should be discouraged from connecting personal devices, such as phones, iPods, tablet computers and flash drives to institutional computer systems.

- Downloading of any material form the Internet should be closely supervised to avoid viruses and potential copyright infringement.

System Intrusion

Computer system intrusion can happen in a variety of ways: access in an unauthorized manner, by an unauthorized user, internally by a member of the institution or externally by the public.

Advanced software can alert a system administrator if an unauthorized access has been attempted. Older systems may require a regular manually review of computer logs to detect unwanted access.

Computer logs and advanced software, if properly configured, can indicate which computer files, if any, have been accessed. A policy should be established to inform members if files containing personal or sensitive information have been exposed. It is likely best to err on the side of caution in such situations.

Unauthorized computer access is potentially a criminal act. System intrusions rarely happen by accident and, as such, it is best to assume the person violating the system is seeking something. As with Website hacking, those perpetrating a system breach, likely know they are breaking the law and may have motivation to justify that risk.

As soon as a system intrusion is detected the system administrator must be contacted immediately. Subsequent contact to law enforcement and FBI (http://www.ic3.gov/default.aspx) computer crime specialists would not be an unusual next step.

Mobile Devices (smartphones, tablets, gaming and media players)

- Due to the recent emergence and proliferation of smart mobile communication devices and mobile computing, there is at this time very little anti-virus or anti-malware protection for mobile computing devices. Mobile devices should only be granted access to institutional systems under the supervision of an experienced service provider, who clearly understands the security needs of a Jewish institution.

Event Response

Website Hacking

Website hacking can take a number of different forms and can happen for a variety of reasons. For this document we are defining a hacking as; activity in the secure section of a Website that is *not* the result of action by an authorized individual. How the hacking occurs is secondary, here we are discussing what to do afterward.

- We suggest contacting the hosting company for the Website as soon as the incident is discovered. The hosting company will need to preserve a copy of the hacked page(s) and copies of all relevant server logs. The hacked page(s) need to be removed as soon as possible in case malware is involved and also to limit the hacker's usual main objective – to gloat.

- Report the event to the police and FBI (http://www.ic3.gov/default.aspx) promptly. Provide them with a copy of the material left by the hacker especially if it involves threats or hateful language.

- Restore the Website from back-up copy of the Website, but only after the hosting company or ISP acknowledges the issues relating to the hack have been addressed.

Distributed Denial of Service Attack (aka DoS attack)

DoS attacks are the simplest and most common form of cyber-attack. A DoS attack is a coordinated effort by a group of computers to request access to a Website. This creates a situation where no one can access the Website or that the contents are delivered very slowly. In many cases a Website hosting company will shut down a Website temporarily rather than create a problem for their other customers. If a Website is the potential target of attacks, the Website hosting company should be made aware of the situation in order to help offer solutions.