Evergreen Islamic Center

IT Security Policy

EIC IT & Communication Team

Evergreen Islamic Center
2486 Ruby Ave
San Jose, CA 95148

TABLE OF CONTENTS

1. Introduction

As **Evergreen Islamic Center** (EIC) has grown over last couple of years, we have had a need to establish a proper IT policy in place to ensure that EIC is equipped with proper tools and resources to handle and safe keep our members' data. This includes donor database, Musallah database and web properties. This Information Security Policy states the types and levels of security over the information technology resources and capabilities that must be established and operated in order for those above mentioned items to be considered secure and in compliance with local regulations. In addition, this document will prescribe ways to handle breaches and security mishaps should they occur.

1.1. Purpose

This Security Policy document defines the security requirements for the proper and secure use of the Information Technology services at EIC. The goal is to protect the **Evergreen Islamic Center** and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation and business outcomes. This document will also outline acceptable IT policies which the users need to adhere.

1.2. Scope

This document applies to all the users in the **Evergreen Islamic Center**, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory for this constituency.

1.3. History

Version	Description	Modified On
1.0 Draft	Initial version	05/07/2018
1.1 Draft	Minor updates, grammar, spelling	08/15/2018
1.2 Draft	Updates based on Br Muneem's questions/suggestions	11/19/2018
1.0 Final	Added definition of Security Officer	11/30/2018

1.4. Responsibilities

Roles	Responsibilities
President	• Accountable for all aspects of the EIC's information security.
Information Security Officer (President or	• Lead the overall effort to manage all aspects of information security • Provide reports to board member

IT/Communication team lead)	• Work with the board to ensure policies are in place and communicated to the EIC general members
IT & Communication Team	• Responsible for the security of the IT infrastructure. • Plan against cyber security threats, vulnerabilities, and risks. Bi-annually do the following: o Run vulnerability assessment o Pen testing o Application security profile for WordPress, EIC released apps • Implement and maintain Security Policy documents. • Ensure security training and awareness programs. • Ensure IT infrastructure supports Security Policies. • Respond to information security incidents. • Help in disaster recovery plans.
Board Members	• Help with establishing the security requirements for their specific area such as finance, web sites, email list etc. • Determine the privileges and access rights to the resources within their areas. • Evaluate and approve proposed policies
Users	• Meet Security Policies. • Report any attempted security breaches.

1.5. General Policy Definitions

1. Exceptions to the policies defined in any part of this document may only be authorized by the Information Security Officer in conjunction with the board approval. In those cases, specific procedures may be put in place to handle request and authorization for exceptions. Exception must be in writing or formal email from the ISO.
2. Every time a policy exception is invoked, an entry must be entered into a security log specifying the date and time, description, reason for the exception and how the risk was managed. This entry may happen via email to the security mailing list which is archived in the cloud.
3. All the IT services should be used in compliance with the technical and security requirements defined in the design of the services.
4. Infractions of the policies in this document may lead to loss of data and EIC reputation. So, all members must be very cognizant of their actions and its impact.

2. IT Assets Policy

2.1. Purpose

The IT Assets Policy section defines the requirements for the proper and secure handling of all the IT assets in EIC. This includes web assets and mailing lists of the donors.

2.2. Scope

The policy applies to desktops, laptops, printers and other equipment, to applications and software, to anyone using those assets including internal users, temporary workers and visitors, and in general to any resource and capabilities involved in the provision of the IT services.

2.3. Policy Definitions for Hardware

1. IT assets must only be used in connection with the EIC activities they are assigned and / or authorized.
2. All the IT assets must be classified into one of the categories in EIC's security categories; according to the current business function they are assigned to.
3. Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
4. All the IT assets must be in locations with security access restrictions, environmental conditions and layout according to the security classification and technical specifications of the aforementioned assets. Example of such a location would be a locked EIC office space in the Mosque.
5. Active desktop and laptops must be secured if left unattended. Whenever possible, this policy should be automatically enforced via screen save and/or auto logoff.
6. Access to assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provision of a service must be done through the approved Service Request Management and Access Management processes. The approval process can be initiated by sending an email to President/IT security officer.
7. All personnel interacting with the IT assets must have the proper training.
8. Users shall maintain the assets assigned to them clean and free of accidents or improper use. They shall not drink or eat near the equipment.
9. Users must not install third party application without the help of the IT team. This will reduce proliferation of virus and malware in the EIC network.
10. Flash drive and portable hard disk should not be used unless the content is fully encrypted.
11. Access to assets in EIC location must be restricted and properly authorized, including those accessing remotely. EIC's laptops, Tablets (iPad/digital equipments) and other equipment used at external location must be periodically checked and maintained.

12. The IT Technical Teams are the sole responsible for maintaining and upgrading configurations. None other users are authorized to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software. This also includes Wi-Fi access, smart hubs, electronic doors and other monitoring devices.
13. Wi-Fi access maybe granted on per user basis. Wi-Fi password must not be displayed publicly anywhere in the property.
14. Special care must be taken for protecting laptops, phones and other portable assets including flash drives from being stolen. Be aware of extreme temperatures, magnetic fields and falls.
15. When travelling by plane, portable equipment like laptops and phones must remain in possession of the user as hand luggage if it contains sensitive data from **Evergreen Islamic Center**.
16. Hard copy of sensitive data such as donor list, financial figures must be kept safely in possession of the board member at all times.
17. Whenever possible, encryption and erasing technologies should be implemented in portable assets in case they were stolen.
18. Losses, theft, damages, tampering or other incident related to assets that compromises security must be reported as soon as possible to the **Information Security Officer**.
19. Disposal of the assets must be done according to the specific procedures for the protection of the information. Assets storing confidential information must be physically destroyed in the presence of an Information Security Team member. Assets storing sensitive information must be completely erased in the presence of an Information Security Team member before disposing.

2.4. Policy Definitions for Web and Other Assets

1. Musallah DB must be backed up regularly on remote site.
2. Access to DB backups should be restricted to IT & Communication team members
3. EIC Election committee should dispose of the list of voters after each election. A centralized system would be designed for EIC Elections in future to reduce burden on the committee.
4. Bank accounts and other financial assets should be guarded with extra care.
    - Web access to bank accounts must be restricted to Treasurer, President and other relevant parties. Account credentials must not be stored or written down in the office which can be easily viewed.
    - Auditing shall be turned on for accessing accounts via web. Notifications of any changes to account shall be sent to board and finance team
    - Account credentials shall be changed every 3 months
5. Applications developed under **Evergreen Islamic Center** banner should be reviewed and tested by communication team and board members willing to participate in the test cycles. The apps include but not limited to:

   - Quranic application for Android and iOS
   - EIC Link app for iOS and Android
   - Others
6. MailChimp account shall be handled by communication team only.
   - Any global email sent to all members must be “Test Sent” to few members including eic-board mailing list for proof reading and approval (see section below for details).
   - Mailing list shall not be exported out of the system without prior discussion and approval of the board.
   - Exported mailing list or CSV file used to batch import users must be deleted upon completion of the task
7. Changing the **Evergreen Islamic Center** Web site:
   - Request for changes to the web site should be sent to EIC communication list
   - Press releases issued by EIC regarding various current events shall be added to the press release specific page on the site with link from main page. Press releases must be approved by the board members prior to posting
   - Changes must be logged with appropriate timestamp and version control
   - Each authorized user must use their own credentials to login and make the change and not use the root account
   - Login credentials shall be changed every three months
   - The web site will deploy SSL for all communications between users and the site

3. ACCESS CONTROL POLICY

3.1. Purpose

The Access Control Policy section defines the requirements for the proper and secure control of access to IT services and infrastructure in the **Evergreen Islamic Center**. Policy of least privileges should be applied at all times. If elevated privilege or access is needed, it can be approved on need per basis.

3.2. Scope

This policy applies to all the users in EIC, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

3.3. Policy Definitions

1. Any system that handles valuable information must be protected with a password-based access control system.

2. Any system that handles confidential information must be protected by a two factor -based access control system.
3. Discretionary access control list must be in place to control the access to resources for different groups of users.
4. Mandatory access controls should be in place to regulate access by process operating on behalf of users.
5. Access to resources should be granted on a per-group basis rather than on a per-user basis.
6. Access shall be granted under the principle of "less privilege", i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform successfully their business functions.
7. Whenever possible, access should be granted to centrally defined and centrally managed identities.
8. Users should refrain from trying to tamper or evade the access control in order to gain greater access than they are assigned.
9. Automatic controls, scan technologies and periodic revision procedures must be in place to detect any attempt made to circumvent controls.

4. Password Control Policy

4.1. Purpose

The Password Control Policy section defines the requirements for the proper and secure handling of passwords in EIC.

4.2. Scope

This policy applies to all the users in EIC, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

4.3. Policy Definitions

1. Any system that handles valuable information must be protected with a password-based access control system.
2. Every user must have a separate, private identity for accessing IT network services.
3. Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
4. Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 8 characters long.
5. Each regular user may use the same password for no more than 90 days and no less than 3 days. The same password may not be used again for at least one year.

6. Password for some special identities will not expire. In those cases, password must be at least 15 characters long.
7. Use of administrative credentials for non-administrative work is discouraged. IT administrators must have two set of credentials: one for administrative work and the other for common work.
8. Sharing of passwords is forbidden. They should not be revealed or exposed to public sight.
9. Whenever a password is deemed compromised, it must be changed immediately.
10. For critical applications, digital certificates and multiple factor authentication using smart cards should be used whenever possible.
11. Identities must be locked if password guessing is suspected on the account.

5. Email Policy

5.1. Purpose

The Email Policy section defines the requirements for the proper and secure use of electronic mail in the Evergreen Islamic Center. Specifically maintaining users lists, donor lists and other email lists which are used for communications.

5.2. Scope

This policy applies to all the users in EIC, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

5.3. Policy Definitions

1. All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of the **Evergreen Islamic Center**. Occasional use of personal email address on the Internet for personal purpose may be permitted if in doing so there is no perceptible consumption in the **Evergreen Islamic Center** system resources and the productivity of the work is not affected.
2. Use of the **Evergreen Islamic Center** resources for non-authorized advertising, external business, spam, political campaigns, and other uses unrelated to the **Evergreen Islamic Center** business is strictly forbidden.
3. In no way may the email resources be used to reveal confidential or sensitive information from EIC outside the authorized recipients for this information.
4. Using the email resources of the **Evergreen Islamic Center** for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the local and state law and ethics is absolutely discouraged.

5. Use of the **Evergreen Islamic Center** email resources is maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the company, the associated account must be deactivated according to established procedures for the lifecycle of the accounts if applicable.
6. Users must have private identities to access their emails and individual storage resources, except specific cases in which common usage may be deemed appropriated. Users may use their gmail accounts to access common shared storage on Google drive. A personal email in eicsanjose.org domain may not be allocated to any user.
7. Privacy is not guaranteed. Mails sent using **Evergreen Islamic Center** official email address are archived and can be viewed by any authorized user permitted to send out mail on behalf of EIC.
8. Identities for accessing **Evergreen Islamic Center** email must be protected by strong passwords. The complexity and lifecycle of passwords are managed by the company's procedures for managing identities.
9. Outbound messages from corporate account should have approved signatures at the foot of the message with **Evergreen Islamic Center's** physical address and phone number.
10. Attachments must be limited in size according to the specific procedures of mail carrier and shall not exceed more than 5mb in size. Files larger than 5mb should be shared using Google Drive. Whenever possible, restrictions should be automatically enforced.
11. Whenever possible, the use of Digital Rights technologies is encouraged for the protection of contents. Powerpoint slides, word documents should have EIC name in preference summary
12. Scanning technologies for virus and malware must be in place in client PCs and servers to ensure the maximum protection in the ingoing and outgoing email.
13. Security incidents must be reported and handled as soon as possible according to the Incident Management and Information Security processes. Users should not try to respond by themselves to security attacks.
14. Corporate mailboxes content should be centrally stored in locations where the information can be backed up and managed according to company procedures. Purge, backup and restore must be managed according to the procedures set for the IT Continuity Management. Initially there will be no deletion of any information artifacts belonging to EIC. Team will still backup documents and other artifacts as needed.
15. IT & Communication team would manage all mailing lists and associated users
    - Mailchimp account credentials should not be shared outside IT & Communication team
    - All emails sent out using info@eicsanjose.org must BCC eic-board@googlegroups.com
    - All emails sent out using info@eicsanjose.org must have signature with EIC's full address and phone number
    - All mass emails must have a link which user can use to unsubscribe from the list. An unsubscribed user must not be added back manually without user's explicit consent
    - All team specific email lists must use eicsanjose@gmail.com as the parent email

6. INTERNET POLICY

6.1. Purpose

The Internet Policy section defines the requirements for the proper and secure access to Internet and acceptable usage.

6.2. Scope

This policy applies to all the users in the **Evergreen Islamic Center**, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

6.3. Policy Definitions

1. Limited access to Internet is permitted for all users using EIC Wi-Fi.
2. Access to questionable sites, hacking sites, and other risky sites is absolutely prohibited.
3. Internet access is mainly for EIC business purpose. –some limited personal navigation is permitted if in doing so there is no perceptible consumption of Evergreen Islamic Center's system resources and the productivity of the EIC business. If in doubt, please ask a board member or IT & Communication team member first.
4. Inbound and outbound traffic must be regulated using firewalls in the perimeter. Back to back configuration is strongly recommended for firewalls.
5. In accessing Internet, users must behave in a way compatible with the prestige of **Evergreen Islamic Center**. Attacks like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
6. Downloading and installing unauthorized software absolutely prohibited. If a driver or software needs to be installed, please request an IT & Communication member for help.
7. Internet traffic should be monitored at firewalls. Any attack or abuse should be promptly reported to the Information Security Officer.
8. Reasonable measures must be in place at servers, workstations and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection and others.
9. Violators maybe suspended from connecting to EIC wi-fi.

7. ANTIVIRUS POLICY

7.1. Purpose

The Antivirus Policy section defines the requirements for the proper implementation of antivirus and other forms of protection in **Evergreen Islamic Center**. EIC sanctioned laptop and desktop must run latest version of anti virus software all the time.

7.2. Scope

This policy applies to servers, workstations and equipment in **Evergreen Islamic Center**, including portable devices like laptops that may travel outside of the **Evergreen Islamic Center** facilities. Some policies apply to external computers and devices accessing the resources of the EIC.

7.3. Policy Definitions

1. All computers and devices with access to EIC network must have an antivirus client installed, with real-time protection.
2. All servers and workstations owned by EIC or permanently in use in EIC facilities must have an approved, centrally managed antivirus. That also includes travelling devices that regularly connects to EIC network or that can be managed via secure channels through Internet.
3. Organization's computers permanently working in other Organization's network may be exempted from the previous rule if required by the Security Policies of the other Organization, provided those computers will be protected too.
4. All the installed antivirus must automatically update their virus definition. They must be monitored to ensure successful updating is taken place.
5. Visitors computers and all computers that connect to EIC's network are required to stay "healthy", i.e. with a valid, updated antivirus installed.
6. Visitors phone and laptop shall connect to "guest" Wi-Fi network only to limit risks to **Evergreen Islamic Center's** computer resources.

8. INFORMATION CLASSIFICATION POLICY

8.1. Purpose

The Information Classification Policy section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality and availability of EIC information.

8.2. Scope

This policy applies to all the information created, owned or managed by EIC, including those stored in electronic or magnetic forms and those printed in paper.

8.3. Policy Definitions

1. Information owners must ensure the security of their information and the systems that support it.
2. Information Security Officer is responsible for ensuring the confidentiality, integrity and availability of EIC's assets, information, data and IT services.
3. Any breach must be reported immediately to the Information Security Officer. If needed, the appropriate countermeasures must be activated to assess and control damages.
4. Information in EIC is classified according to its security impact. The current categories are: **confidential, sensitive, shareable, public and private**.
5. Information defined as ***confidential*** has the highest level of security. Only a limited number of persons must have access to it. Management, access and responsibilities for confidential information must be handled with special procedures defined by Information Security Management.
6. Information defined as ***sensitive*** must be handled by a greater number of persons. It is needed for the daily performing of jobs duties, but should not be shared outside of the scope needed for the performing of the related function.
7. Information defined as ***shareable*** can be shared outside of the limits of EIC, for those clients, organizations, regulators, etc. who acquire or should get access to it.
8. Information defined as ***public*** can be shared as public records, e.g. content published in the company's public Web Site.
9. Information deemed as ***private*** belongs to individuals who are responsible for the maintenance and backup.
10. Information is classified jointly by the Information Security Officer and the Information Owner.
11. Examples of classification
    - **Public**: Any information posted on EIC's web site. Typical posting may include event announcement and various press releases
    - **Shareable**: Any information shared with other organization of similar stature. Such as sharing a resolution accepted by the board for inter organization collaboration.
    - **Private**: Only accessible based on per need basis. Various credentials to access services and resources will fall under this category.
    - **Sensitive**: List of EIC members which can not be shared outside or even with EIC community members. This list may contain email, phone and other means of communication to the member and must be safe guarded
    - **Confidential**: Finance information, donor details such as money contributed would be classified as confidential. This type of information should be handled in **safe place** and unless absolutely necessary, should not be printed and shared

physically with others. Loss of data from this list can cause irreparable damage to **Evergreen Islamic Center's** reputation. When handling this data, multiple people should handle it and in the safe office setting. Laptop, where the data is stored should have full encryption turned on and must have separate credentials for authorized users to login and view the data. Board members can view/review the data in board meetings as presented by the Treasurer and/or President.

9. Remote Access Policy

9.1. Purpose

The Remote Access Policy section defines the requirements for the secure remote access to EIC's internal resources. In general, there should not be a need to connect to internal resources from outside of **Evergreen Islamic Center's** network. Exception is connecting to Musallah database over RDP.

9.2. Scope

This policy applies to the users and devices that need access EIC's internal resources from remote locations. Other than Musallah database, there should not be any need to connect to internal network from outside.

9.3. Policy Definitions

1. To gaining access to the internal resources from remote locations, users must have the required authorization. Remote access for an employee, external user or partner can be requested only by the Manager responsible for the information and granted by Access Management.
2. Only secure channels with mutual authentication between server and clients must be available for remote access. Both server and clients must receive mutually trusted certificates.
3. Remote access to confidential information should not be allowed. Exception to this rule may only be authorized in cases where is strictly needed.
4. Users must not connect from public computers unless the access is for viewing public content.
5. When available a VPN solution shall be used by the connecting user. In lieu of that, secure RDP may be used.

10.Outsourcing Policy

10.1. Purpose

The Outsourcing Policy section defines the requirements needed to minimize the risks associated with the outsourcing of IT services, functions and processes. Albeit, we do not anticipate any outsourcing of IT/Web functions to an external third party at this time. This section is here to cover future efforts should there be a need.

10.2. Scope

This policy applies to EIC; the services providers to whom IT services, functions or processes are been outsourced, and the outsourcing process itself.

10.3. Policy Definitions

1. Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
2. Whenever possible, a bidding process should be followed to select between several service providers.
3. In any case, the service provider should be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties.
4. Audits should be planned in advance to evaluate the performance of the service provider before and during the provision of the outsourced service, function or process. If EIC has not enough knowledge and resources, a specialized company should be hired to do the auditing.
5. A service contract and defined service levels must be agreed between EIC and the service provider.
6. The service provider must get authorization from EIC if it intends to hire a third party to support the outsourced service, function or process.

11. ANNEX

11.1. Glossary

Term	Definition
Access Management	The process responsible for allowing users to make use of IT services, data or other assets.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Confidentiality	A security principle that requires that data should only be accessed by authorized people.

Term	Definition
External Service Provider	An IT service provider that is part of a different organization from its customer.
Identity	A unique name that is used to identify a user, person or role.
Information Security Policy	The policy that governs EIC's approach to information security management
Information Security Officer	A member of the EIC board or general member who has been chosen by the EIC board to lead EIC IT policy management and implementation.
EIC	Evergreen Islamic Center
Outsourcing	Using an external service provider to manage IT services.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc.
Risk	A possible event that could cause harm or loss, or affect the ability to achieve objectives.
Service Level	Measured and reported achievement against one or more service level targets.
Warranty	Assurance that a product or service will meet agreed requirements.

Table 1. Glossary.

Board Acceptance v 1.0
Nov 30, 2018