Cyber security policy

Policy Brief & Purpose

This cyber security policy is dedicated to El Hassan Youth Award, follows the Cybercrime Law No. 27 of 2015, outlining our steadfast commitment to safeguarding the digital integrity of our data and technological resources. As an initiative deeply engaged in youth empowerment and development, we increasingly depend on technology to amass, store, and manage sensitive information. This reliance elevates our exposure to potential security breaches, this may include human errors, cyber-attacks, and system failures.

Recognizing these vulnerabilities, we are proactive in preserving the confidentiality and integrity of participant data, financial records, and strategic information. These are not just operational necessities but also a matter of maintaining the trust placed in us by our community and stakeholders.

To fortify our defense against risks, we have instituted a comprehensive set of security measures. These encompass robust protocols for data protection, stringent guidelines for technology use, and best practices for digital communication. Additionally, we provide clear, actionable instructions to mitigate cybersecurity risks, fostering a culture of awareness and responsibility among all those associated with El Hassan Youth Award.

This policy encapsulates both our security frameworks and procedural directives. It is crafted not just as a guideline but as a testament to our unwavering commitment to cybersecurity in the pursuit of excellence in youth development.

Scope

This cyber security policy is applicable to everyone associated with the El Hassan Youth Award. This includes, but is not limited to, our staff, volunteers, Award Leaders, contractors, and any individuals who have permanent or temporary access to Online Record Book (ORB) system and hardware. Whether directly involved in the Award programs or in a supporting role, all individuals must adhere to the guidelines set forth in this policy to ensure the highest level of data protection and system integrity.

Policy elements

Confidential data

Confidential data refers to any information that is crucial to our operations and that must be kept secure to protect the interests of our participants, partners, and the integrity of our programs. Common examples of confidential data relevant to our setting include:

- This include but not limited to personal information of participants and volunteers, or other stakeholders such as Name, contact details, Award Leader and personal achievements.
- Sensitive details about our youth programs, including internal strategies and participant evaluations.
- Financial information related to the Award's funding, sponsorships, and allocation of resources.
- Communications and correspondences with partners, sponsors, and stakeholders.
- Proprietary information related to the methodologies and technologies employed in our youth development initiatives.

All employees or contractors are obliged to protect this data, if they have access to it. In this policy, we will give our employees instructions on how to avoid security breaches.

Protect personal and company devices

When individuals affiliated with El Hassan Youth Award use their digital devices to access Award-related emails or accounts, they introduce a potential security risk to our sensitive data. We strongly advise everyone involved in the Award - including staff, volunteers, and participants - to maintain the security of both their personal and any Award-issued digital devices (computers, tablets, and cell phones).

They can enhance security by:

- Keeping all devices password-protected with strong, unique passwords.
- The IT department is responsible for continuously to select and regularly updating comprehensive antivirus software.
- Ensuring their devices are never left exposed or unattended in public spaces.

- Installing security updates for browsers and operating systems promptly.
- Accessing Award-related accounts and systems exclusively through secure and private networks.

Additionally, we recommend avoiding the use of other people's devices for accessing Award-related systems and refraining from lending their devices to others for such purposes.

New participants or staff receiving Award-issued equipment will be provided with instructions for:

- Setting up disk encryption to protect data stored on the device.
- Using a password management tool to maintain robust password security.
- Following up with the IT department to continuously install and update antivirus/anti-malware software to protect against threats.

It is vital that all instructions are followed diligently to protect the devices. For any queries or assistance, individuals should reach out to our designated Security Specialists or IT department.

Keep emails safe

Email communication is a vital tool in El Hassan Youth Award's operations, but it can also be a gateway for scams and malicious software (such as worms). To prevent virus infections or data theft, we urge all individuals associated with the Award – staff, volunteers, and participants – to exercise caution and adhere to the following guidelines:

- Avoid opening email attachments or clicking on links if the content is vaguely described (e.g., messages like "Check out this amazing video!" without further context).
- Remain skeptical of sensational or clickbait titles that promise prizes, shocking news, or unsolicited advice.
- Verify the email addresses and names of senders to ensure that the messages are from legitimate sources.

- Look out for red flags in emails, such as poor grammar, unnecessary use of capital letters, or an excessive number of exclamation marks, which might indicate phishing attempts.

In case of uncertainty regarding the safety of an email, individuals should not hesitate to consult with our designated IT Specialist. It's always better to be cautious and seek confirmation rather than risk compromising personal or Award-related information.

Manage passwords properly

Password security is crucial in safeguarding El Hassan Youth Award's digital infrastructure. Weak or compromised passwords pose a significant threat, potentially endangering the entire network and sensitive information related to our youth programs. Therefore, we strongly advise everyone involved in the Award to:

- Create robust passwords with a minimum of eight characters, including a mix of uppercase and lowercase letters, numbers, and symbols. Avoid using easily guessable information, such as birthdays or common words.
- Memorize passwords rather than writing them down. If it is necessary to write down a password, it must be kept in a highly secure manner and properly destroyed once it is no longer needed.
- Share credentials only when absolutely essential. If in-person sharing isn't feasible, prefer a phone conversation over email for exchanging such information, and ensure you recognize the person you are communicating with.
- Regularly update passwords, ideally every two months, to maintain security.

Given the challenge of remembering multiple complex passwords, when necessary El Hassan Youth Award will provide access to a reputable password management tool. This tool will assist in generating and storing secure passwords. Each individual will be responsible for setting a strong, unique password for accessing this tool, adhering to the guidelines mentioned above.

Transfer data securely

When necessary transferring data, especially sensitive information related to youth programs, introduces significant security risks. It is imperative for everyone involved in El Hassan Youth Award – including staff, volunteers, and partners – to adhere to strict data transfer protocols to maintain the integrity and confidentiality of our information. Accordingly, individuals must:

- Refrain from transferring sensitive data (such as participant information, program details, and internal records) to other devices or accounts unless it is absolutely necessary. For large-scale data transfers, we request that you seek assistance from our Security Specialists and IT department to ensure safe and secure handling.
- Share confidential data exclusively over the Award's secure network/system. Avoid using public Wi-Fi or private connections that are not verified for security.
- Verify that the recipients of the data are appropriately authorized and equipped with adequate security measures to handle the information responsibly.
- Promptly report any suspicious activities, privacy breaches, and hacking attempts.

It is crucial for our IT Specialists/IT department to be informed about potential threats such as scams, breaches, and malware to enhance our defenses. Therefore, we urge everyone to report any perceived attacks, suspicious emails, or phishing attempts immediately to our specialists. Our IT team is responsible for investigating these reports promptly, resolving any issues, and issuing a company-wide alert if necessary.

Our Security Specialists and IT department are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional measures

To minimize the risk of security breaches in the context of El Hassan Youth Award, we instruct all individuals involved - including employees, volunteers, and any other stakeholders - to:

- Ensure their screens are turned off and their devices are locked when stepping away from their workstations.
- Promptly report any stolen or damaged equipment to the HR or IT Department.
- Immediately change all account passwords if a device associated with the Award is stolen.
- Alert the IT team about any perceived threats or potential security weaknesses in our systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on any devices used for award-related activities.
- Avoid accessing suspicious websites and adhere to our social media and internet usage policies.

Our Security Specialists/Network Administrators are tasked with:

- Implementing and maintaining robust firewalls, anti-malware software, and access authentication systems.
- Organizing regular security training sessions for all individuals involved in the Award to enhance awareness and preparedness.
- Keeping everyone informed about new scam emails, viruses, and effective methods to counteract them.
- Conducting thorough investigations into any security breaches.
- Adhering to this policy's provisions, setting an example for all other staff and volunteers.

El Hassan Youth Award is committed to maintaining the highest standards of digital and physical security to protect our information and the individuals we engage with.

Remote employees

Remote participants and staff and Award Leaders or anyone might work remotely with El Hassan Youth Award or any one working remotely also required to rigorously follow the guidelines outlined in this cyber security policy. Given that they will be accessing Award-related accounts and systems remotely, it is crucial for them to adhere to all data encryption and protection standards set by the award. They must ensure that their private

network is secure and protected against unauthorized access and contact the offices for any assistance or report any concerns immediately, we strongly encourage remote individuals to:

- Maintain the security of their private Wi-Fi networks, using strong, unique passwords and implementing network encryption.
- Be vigilant about the physical security of their devices, especially when working in public or shared spaces.
- Stay updated with the latest security protocols and software updates as recommended by the Award.

In case of any doubts or need for assistance, remote staff and participants should not hesitate to seek advice from our Security Specialists or IT Administrators. These professionals are equipped to provide guidance and support to ensure that remote access to Award systems is as secure as possible

Disciplinary Action

We hold all participants, staff, Award Leaders , volunteers, …etc to the highest standards of cyber security compliance. It is imperative that everyone adheres to this policy, and failure to do so may result in disciplinary action:

Minor, Unintentional Security Breach: In cases of a first-time, unintentional, and small-scale security breach, we may issue a warning. The individual may also receive additional training on security protocols to prevent future occurrences

Intentional, Repeated, or Large-Scale Breaches: More severe breaches, particularly those that are intentional, repeated, or cause significant financial or reputational damage to the Award, will result in stricter disciplinary actions. These actions may extend up to and including dismissal from the program or termination of employment and in some cases felony charge.

Each incident will be evaluated on a case-by-case basis, taking into consideration the context and severity of the breach.
Furthermore, consistent disregard for our security instructions, even in the absence of a direct security breach, will not be tolerated. Such behavior will be subject to progressive discipline to reinforce the importance of adhering to our cyber security policies.

Take security seriously

In the realm of El Hassan Youth Award, everyone from participants, staff, and volunteers to our partners and supporters, plays a pivotal role in ensuring the safety of data. The trust and safety of our participants and stakeholders are paramount. The only way to uphold and strengthen this trust is by proactively safeguarding our systems and databases against cyber threats. We all contribute to this mission by remaining vigilant and consistently prioritizing cybersecurity in all our activities and interactions.

Disclaimer: This policy is designed to provide general guidelines and serve as a framework for the El Hassan Youth Award. It is intended as a reference and may not encompass all relevant local and international law but in adhere to them. This document is not a legal instrument, and neither the authors nor the organizers of El Hassan Youth Award will assume any legal liability that may arise from the use of this policy. For specific legal advice or assistance, please consult with a qualified legal professional.

Contact Information

For any questions, concerns, or requests related to your personal data and privacy, please contact us at:
El Hassan Youth Award Office:
Location: Amman- Al Jubaiha- Ahmad Al Tarawneh St –building 84
Phone: 065356695
Email: info@hyaward.org.jo
P.O. Box 840908 Amman 11180 Jordan

Cyber Security Lead at Board Level:
Name: Dr, Khawla Alhasan
Email: dataprotection@hyaward.org.jo
Phone: 0797611796