ANND Digital Policy

April 28th, 2024

annd
Arab NGO Network
for Development
شبكة المنظمات العربية
غير الحكومية للتنمية

Table of Contents

Executive Summary:

The digital policy for ANND serves as a comprehensive framework to manage digital risks, ensure compliance with regulations, and promote responsible engagement with digital platforms, yet, not hinder staff nor target audience from actively engaging with the digital platforms. It emphasizes accountability, awareness, and knowledge of digital practices among staff, aiming for informed, secure, and compliant digital operations within the organization. Key elements of the policy include risk management, which involves mitigating cybersecurity threats and data breaches through regular risk assessments and implementing measures such as endpoint security software, encryption, and secure remote access.

Additionally, staff training and awareness are prioritized, with comprehensive training on policy requirements provided through interactive workshops, online courses, and tailored sessions for different organizational roles. Compliance is enforced through clear communication, monitoring, and enforcement mechanisms, including regular compliance checks, agreements, and consequences for non-compliance. Data protection principle emphasize lawfulness, fairness, transparency, and integrity in processing and safeguarding personal data. Guidelines for digital platforms cover content shared on social media, incorporating risk analysis, accuracy, consent, and maintaining a consistent brand identity. Staff are encouraged to exercise caution when using personal platforms, with disclaimers to differentiate personal views from organizational ones.

The policy also includes provisions for monitoring and managing the organization's online reputation, including response mechanisms and consulting management for appropriate actions. Moreover, this policy dedicates a section to ensure access for people with disabilities.

The drafting and eventual implementation of the ANND digital policy aim to foster a culture of ethics, accountability, and responsible digital practices within ANND, and ultimately safeguarding the organization's integrity, reputation, and data security.

Introduction

The implementation of this policy’s regulations will ensure accountability, and foster a culture of awareness and knowledge of digital practices within an organization which will in turn lead to informed, responsible, secure, and compliant digital practices within the organization.

The role of the digital policy is to create awareness and compliance with the digital regulations installed by ANND as everyone within this organization is accountable and play a vital role in maintaining the organization's culture, integrity, and reputation.

The following main points of this digital policy will be expanded further to constitute a reference for the digital use and application.

Risk Management

Mitigate cybersecurity threats and data breaches when applying communication by conducting regular risk assessments to identify potential vulnerabilities in the organization's digital infrastructure, systems, and processes which include:

Endpoint Security Software: Require staff to install and regularly update endpoint security software, such as antivirus and anti-malware programs, on their personal laptops. This helps protect against threats like viruses, ransomware, and other malicious software.

Encryption: Encourage or mandate the use of encryption tools to encrypt data stored on personal laptops. Full disk encryption and encryption of sensitive files and folders can prevent unauthorized access to data in case the laptop is lost or stolen.

Remote Wipe and Data Loss Prevention (DLP): Implement remote wipe capabilities to remotely erase data from personal laptops in case they are lost or stolen. Additionally, consider implementing Data Loss Prevention (DLP) solutions to monitor and control the transfer of sensitive data to personal devices.

Strong Authentication: Enforce strong authentication mechanisms, such as multi-factor authentication (MFA), to ensure that only authorized users can access organization data and systems from personal laptops.

Regular Updates and Patch Management: Require staff to keep their personal laptops up to date with the latest operating system patches, security updates, and software upgrades. Regular updates help address known vulnerabilities and reduce the risk of exploitation by cyber threats.

Secure Remote Access: Use secure remote access technologies, such as virtual private networks (VPNs) and secure sockets layer (SSL) connections, to enable staff to access organization resources securely from their personal laptops. Ensure that remote access is encrypted and authenticated to prevent unauthorized access. One good example would be the setting up of the professional router. ANND has and which provides secure access through VPN connection and SSL.

Secure Communication Platforms: Choose communication platforms that prioritize security and offer features such as encryption, access controls, and audit trails. Platforms like encrypted messaging apps, secure video conferencing tools, and collaboration software with built-in security features help protect remote communication channels.

Secure File Sharing: Implement secure file sharing solutions that allow users to share and collaborate on documents securely. This includes encryption of files in transit and at rest, access controls, and the ability to revoke access to shared files if necessary.

Regular Security Audits and Assessments: Conduct regular audits and security assessments of remote communication systems and practices to identify vulnerabilities, weaknesses, and areas for improvement. This proactive approach helps to strengthen security posture and mitigate risks.

Staff Training and Awareness: Provide training and awareness programs to educate staff about the risks associated with using personal laptops for work and the importance of adhering to security policies and best practices. Ensure that the staff understand their responsibilities in protecting organization data.

Agreements and Consent: Require staff to sign agreements or consent forms acknowledging their understanding of and compliance with the organization's BYOD policy and data protection measures. This can help mitigate legal risks and hold personnel accountable for adhering to security requirements.

In addition, other factors should be considered that can also play a factor in mitigating cyber security risks, including:

Incident Response Plan, and outlining procedures for detecting, reporting, and responding to cybersecurity incidents; it is crucial here to establish clear roles and responsibilities for incident response team members and conduct regular drills to test the effectiveness of the plan. Another key factor is the continuous monitoring and threat Intelligence to emerging cybersecurity threats in real-time, and keeping up-to-date with the latest trends and tactics used by cyber attackers to adapt security measures accordingly.

This would apply to systems and devices of the staff members who use their personal laptops and other electronics for work purposes, deciding if this is the best available option, and if so ensuring that a Bring your own Device (BYOD) policy is put into place.

Compliance

Ensuring compliance is a main factor in the success of the digital policy intended goals. Ensuring the adherence of staff to the regulation is only applicable when they have direct access to the knowledge and information in the policy, as well as a definitive clear grasp of all the main points mentioned.

Therefore, and to ensure adherence to relevant guidelines and regulations the following steps should be put into action:

Clear Communication: management or designated individuals should clearly communicate policy guidelines and expectations, via meetings, workshops and follow ups with an evaluation of the relayed information.

Training and Education:

1. Interactive Workshops: Host interactive workshops where the staff can learn about the digital policy requirements through activities, case studies, quizzes and games, and group discussions.

2. Online Courses: Develop online courses or modules that cover various aspects of digital policies, including data privacy, security protocols. Staff can complete these courses at their own pace, and assessments can be included to ensure understanding.

3. Specific training courses as per position: Tailor training according to personnel's position and TOR within the organization. Different departments may have unique digital policy requirements, so tailoring the training content to specific roles ensures relevance and applicability.

4. Experts and guest speakers: They can share relatable information and case studies drawn from their experience

5. **Regular Refreshers:** Digital policies are constantly evolving; therefore, it is necessary to provide regular updates and refresher training sessions to ensure staff stay informed about any changes or new requirements.

6. **Feedback Mechanisms:** Establish feedback mechanisms where staff can ask questions, provide input, or report issues related to digital policies. This fosters a culture of continuous learning and improvement.

7. **Compliance Checks:** Conduct regular compliance checks or audits to ensure the staff are adhering to digital policy requirements. Use these checks as opportunities to identify areas for additional training or reinforcement.

Acknowledgement and Agreement: Require staff to acknowledge and agree to comply through specific documents they can read, understand, and sign

Regular Communication: Send periodic reminders and updates about the policy.

Monitoring and Enforcement: this can be implemented through software solutions designed to streamline and enhance the process of ensuring adherence to regulatory requirements, organizational policies, and industry standards. Moreover, the enforcement process is enhanced by automatically applying preventative measures to non-compliance such as access restrictions when violations occur. Appointing a person or more to closely follow up on the digital platforms of the organization to ensure compliance with the digital policy

Consequences for Non-Compliance: Clearly outline repercussions for violations.

Promote a Culture of Compliance: Foster a culture where compliance is valued.

Anonymous Reporting Mechanism: Provide a way for staff to report violations anonymously.

Leadership Example: Lead by example, demonstrating commitment to compliance.

Data Protection

The General Data Protection Regulation[2] formulated by the EU is the advised method to apply when seeking data protection; the GDPR aims to protect the personal data of individuals by establishing regulations that govern the collection, processing, and storage of such data. It also enhances and prioritizes users' rights and privacy. In this policy we will address the main following principles that staff is advised to adhere to and implement in the process of data protection within the organization:

Lawfulness, Fairness, and Transparency: ANND must have basis for processing data, informing individuals about how their data will be used, and ensuring that processing is fair to individuals.

Purpose Limitation: the purposes for which data is collected must be clearly stated, and then adhered to.

Data Minimization: Personal data collected should be sufficient, relevant, and restricted to what is necessary to achieved the defined purpose. Collecting excessive or unnecessary data should be avoided.

Accuracy: Personal data should be accurate and kept up to date to avoid unnecessary mistakes that can prompt legal action.

Storage limitation: Outdated data should either be updated or deleted when it no longer serves the organization

Integrity and Confidentiality: ensure modes of safeguarding data against unauthorized, unlawful processing and accidental loss, destruction, or damage.

Digital Platforms Regulations

All staff including those who post only on their own platforms can undergo an orientation on the use of social media. Clear guidelines for the use of digital platforms should be shared with all staff and include the following:

When content is shared on social media, it's crucial to ensure that it adheres to certain guidelines to maintain professionalism and avoid legal issues:

Risk analysis: a general assessment of the content that is to be shared should be analyzed for, containing any risk that can create a backlash, be misused by a group against another, or whether it is considered inflammatory. Other considerations may be also added by the communications team. The analysis is not to restrict the sharing of content, but rather to either adjust content to minimize any negative reactions and comments, and to be fully prepared in the case that contents benefits outweigh its risks, and which usually happens when advocating for a cause.

Published Content: Content must be free from inflammatory language, hate speech, racism, or discrimination of any kind. A Questions and answers (Q&A) sheet should be developed, that includes most common questions that the audience puts forth and in which the answers are unified and utilized by all staff that manage community engagement, to ensure engagement in an optimal manner and that is previewed and cleared by management.

Accuracy and Fact-Checking: Ensure that information shared on social media is accurate and fact-checked to maintain credibility and avoid spreading misinformation.

Use of images, photos, videos or other multimedia material: when using images, photos, videos or other multimedia material on the digital platforms of an organization, they should be either licensed, or produced inhouse. If the material's source is unknown, usage should be avoided. Certain materials available online are free for public use and in this case, a clearance is required by management to ensure no copyright infringement.

Obtaining Consent: staff should refrain from sharing information and images about individuals without their written and signed consent prior to posting the info. A consent form explaining where the content will feature and that the organization cannot contain the spread of the image or info once it is online should be clearly communicated and stated on the form.

Use of Personal Platforms

Staff should refrain from associating the name of the organization with their personal social platforms. This is the best measure to ensure that the content and images they share is not impact the organization. Another measure could be a disclaimer that clearly states that content and visuals shared expresses entirely their own views and does not reflect the organization’s views in any shape or from. This will also allow the staff autonomy of self-expression without harming the reputation of the organization.

Consistent Messaging & Branding

A consistent tone and visual identity across all communication channels, such as logo, colors, typography, and imagery will foster a strong and memorable brand identity. This makes it easier for the audience and stakeholders to recognize the organization, and reinforce the organization's mission and range of services. In addition, this consistency ultimately reflects the organization’s professionalism and commitment to quality, which in turn, inspires trust and resonates with the stakeholders.

Monitoring and Managing Online Reputation

Monitor on a regular and assigned basis the online sites and news outlets, for mentions of the organization. A response mechanism should be established in order to be able to promptly respond to positive and negative feedback and address misinformation or negative opinions. However, management should be consulted as it is imperative to decide whether the organization will choose to respond in the first place, depending on risk analysis.

People with Disability Access to Digital Tools

Customizable Settings: Allow users to customize the settings and preferences of digital tools to suit their individual needs. This could include adjusting font sizes, color schemes, audio settings, and other elements to enhance readability, visibility, and usability for users with different abilities.

Accessibility Features: Incorporate built-in accessibility features into digital tools, such as screen readers, magnification options, and high-contrast modes. These features enable users with visual impairments to navigate interfaces and consume content more easily.

Keyboard Navigation: Ensure that digital tools can be fully navigated and operated using keyboard shortcuts and commands. This allows users with mobility impairments or dexterity issues to interact with the interface without relying on a mouse or touch input.

Alternative Input Methods: Provide support for alternative input methods, such as voice commands, gesture controls, or switch devices. These options cater to users with limited mobility or motor control, allowing them to interact with digital tools in ways that are comfortable and accessible.

Descriptive Text and Alternative Media: Ensure that all content within digital tools is accompanied by descriptive text and alternative media formats, such as audio descriptions for videos and image alt text. This provides users with visual or hearing impairments access to the same information and functionality as other users.

annd
Arab NGO Network
for Development

شبكة المنظمات العربية
غير الحكومية للتنمية

www.annd.org