Global Information Technology Policies and Procedures Manual

Table of Contents

Acceptable Use Policy

Company Equipment	**Policy Effective Date:** 1 November 2017
	Department of Origin: IT
	Policy Number: IT.GL.01

PURPOSE

This document provides the policy and procedures regarding the use of Company Equipment, the proper care and operation of Company Equipment, and the security therein. The purpose of this policy is to ensure the longevity, security, reliability, and cost-effectiveness of company assets. This policy applies to all Evidence Action employees.

POLICY AND PROCEDURES

Company Equipment is the property of Evidence Action and is intended to be used for Evidence Action business. Employees are expected to use Company Equipment in the completion of their duties. Occasional incidental personal use is normal and permitted. Excessive personal use of Company Equipment, including activity that is damaging to Company Equipment or systems, or activity that is illegal or puts the company at risk is strictly prohibited.

Improper use of any equipment or systems may subject Evidence Action to serious consequences, including negative public perceptions and legal actions. Any prohibited activity will subject the violator to corrective action as defined by the pertinent Human Resources policy.

Employees are responsible for the safety and security of the Company Equipment that they are issued. Company Equipment in the possession of an employee is the employee's responsibility, and is to be treated with appropriate care and precaution to avoid unauthorized access, damage, loss or theft. If Company Equipment is damaged, stolen, or rendered unusable, the employee must notify their immediate supervisor and the IT department as soon as possible.

Company Equipment must be secured with a unique username and password that adheres to the Passwords and Authentication Policy. See IT.GL.05 for more detail. Employees must sign off or lock workstations when the system is left inactive or unattended. Unauthorized access to a laptop, phone or device that is logged into an Evidence Action system constitutes a potential breach in company safeguards. Employees should maintain visual and physical control of Company Equipment while traveling.

Employees are not permitted to download software requiring administrative access to Company Equipment without consultation with the IT department.

Company Equipment in use by an employee is to be returned upon completion of their employment.

All Company Equipment must have up-to-date Antivirus, Antimalware, Endpoint Security and Management Software installed and actively protected. This is the responsibility of the IT department.

The use of personal devices is allowed at Evidence Action subject to the guidelines found in the Bring Your Own Device Policy (IT.GL.06).

Procurement of equipment such as laptops, monitors, printers, and computers will be as standardized as possible to ensure consistency with the brand and model of equipment used at Evidence Action. The IT department will provide guidance on the specifications, brand, model, and pricing of equipment to be procured. While availability of equipment can vary by locality, all attempts should be made to conform as closely as possible to the recommended equipment. When purchasing equipment such as laptops, it is strongly advised to secure a warranty of 3 years or more to match the anticipated useful life span of the equipment.

All laptops, computers, tablets, smartphones, printers and other equipment should be recorded and tracked in an equipment/asset inventory. This is the responsibility of the IT department with support from administrative staff in some regions. Pertinent equipment data that is captured should include manufacturer, model, serial numbers, purchase data, system hardware configuration, software configuration, operating system, general specs, warranty information, employee assignment, physical office location, and any other relevant notes regarding purchase date, access or usage.

All laptops, computers, tablets or smartphones procured by Evidence Action must have an asset tag affixed. This is the responsibility of the IT department with support from administrative staff in some regions. The asset tag's unique number should be recorded in the centralized equipment/asset inventory.

No individual should access Company Equipment without prior approval from the employee, and will only use Global IT recommended solutions to access Company Equipment. At this time Global IT only allows Kaseya's "Remote Control" to access end user computers. Kaseya's "Live Connect" or any other Remote Desktop solution is not permitted. Any exception must require a written approval from the Global IT Director.

A routine cybersecurity monitoring is not part of the scope of this policy.

DEFINITIONS

Company Equipment – any computer, laptop, mobile phone, tablet, or other physical asset that is owned by Evidence Action.

Antivirus – Software designed to detect and eliminate computer viruses.

Antimalware – Software designed to prevent, detect and remediate malicious programming on individual computing devices and IT systems.

Endpoint Security and Management Software – a tool enabling the unified security and administration of company computing equipment including features such as hardware & software inventory, patch management, mobile device management, operating system and software deployments

FURTHER INFORMATION

For additional information, please contact the IT Department.

HISTORY

Origin: 16 August 2017
Last Updated: 15 July 2022, 10 September 2023

Email & Electronic Communication	**Policy Effective Date:** 1 November 2017
	Department of Origin: IT
	Policy Number: IT.GL.02

PURPOSE

This document provides the policy and procedures surrounding the appropriate use of Email and electronic communications within Evidence Action. This policy serves to define specific standards regarding the use of Email and Communication Systems within Evidence Action. The creation and enforcement of these standards protects the interests of Evidence Action, enables more effective and efficient communication, and creates a more respectful working environment. Every Evidence Action employee is responsible for using the Email and Communication Systems properly in accordance with this policy. This policy applies to all Evidence Action employees.

POLICY AND PROCEDURES

Evidence Action Email and other Communication Systems must only be used for Evidence Action-related correspondence. Personal or other non-work related email and messages should be conducted with a separate, personal account.

Employees should be courteous to others and always conduct themselves in a cordial and professional manner. Employees should write electronic communications with no less care, judgment and responsibility than they would use for letters or internal memoranda written on Evidence Action letterhead.

Evidence Action Email or other Communication Systems shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, physical characteristics, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

Evidence Action's policies against sexual or other harassment and bullying as established in the Global Human Resources Policy Manual apply fully to the use of any of these devices and systems.

Evidence Action systems shall not be used to send or receive unauthorized Copyrighted materials, trade secrets, proprietary financial information, credit card information, personal information (i.e. social security numbers, banking or credit card information), donor records, or similar Confidential information as defined in the Information Classification and Security Policy. If employees are uncertain about whether certain information is copyrighted, proprietary, or otherwise inappropriate for transfer, they should resolve all doubts in favor of not transferring the information and consult their immediate supervisor.

Evidence Action data and files are the property of Evidence Action and shall only be emailed, shared, or otherwise transferred in accordance with the Information Classification and Security Policy. Evidence Action has the right to retrieve and read any electronic messages on its system. All Email should be treated according to the Information Classification and Security Policy by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any Email messages or other forms of electronic communication that are not sent to them.

Third party communication tools such as WhatsApp, SMS (text messages), or Skype are not official Evidence Action systems, are not owned by Evidence Action, and may not be secure. In many scenarios these communication tools can prove more convenient or efficient than traditional methods when working in remote areas or with limited

connectivity. However, these tools are to be used with caution, infrequently, and only for informal group chats. Employees should be mindful that these records of communication exist outside of the Company and should thus be treated as public.

Because Evidence Action has a variety of communication channels available to employees, an understanding of their general use is important. While many of these channels are available to employees, teams or departments will set the preference for their particular usage. Please see "Appendix A. Communications Systems in Use at Evidence Action".

Violations of this policy may result in disciplinary action up to and including discharge. Any employee who suspects misuse or discovers misuse of an Evidence Action system should immediately contact the IT Department.

DEFINITIONS

Email – Messages distributed by electronic means from one computer user to one or more recipients via the Internet and a distributed network.

Communication Systems – Refers to any electronic system or device that can be used for communications and messaging within (or external to) Evidence Action. This includes but is not limited to Email, Slack, Skype, Google Hangouts, WhatsApp, comments within documents, etc.

Instant Messaging – Examples of Instant Messaging (IM) systems in use at Evidence Action include Slack, Google Hangout, Skype, and others. IM is a fast, "low friction" form of communication, to avoid the delays of email or voicemail when you need to convey important or time-sensitive information.

Copyrighted Material – May include software, music, movies, files, graphics, documents, messages, and other material.

FURTHER INFORMATION

For additional information, please contact the IT Department.

HISTORY

Origin: 16 August 2017
Last Updated: 1 December 2021

Use of Internet & Computer Resources	**Policy Effective Date:** 1 November 2017
	Department of Origin: IT
	Policy Number: IT.GL.03

PURPOSE

This document provides the policy and procedures regarding the proper use of the Internet at Evidence Action. This policy applies to the use of the Internet from Evidence Action devices, offices, or Evidence Action-supplied Internet access points. This policy defines the guidelines surrounding the proper use of computer resources and specifies activities deemed prohibited. Use of the Internet via Evidence Action's computer system constitutes consent by the user to all of the terms and conditions of this policy.

The purpose of this policy is to safeguard Evidence Action's computers, systems and other electronic resources from abuse, misuse and unnecessary exposure to risk. This policy also helps safeguard against legal liability from inappropriate usage of the Internet.

This policy applies to all Evidence Action employees.

POLICY

Employees are provided with access to a computer and the Internet to assist them in performing their jobs. Internet access is for Evidence Action business purposes.

The Internet can be a valuable source of information and research. However, the Internet presents the company and all users with new risks that must be addressed to safeguard our systems and data. Best practices around Internet usage and cybersecurity awareness should be followed.

Employee use of Evidence Action systems, equipment, and Internet will be monitored. Inappropriate sites will be blocked.

DEFINITIONS

Wifi – A facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

Copyrighted Material – May include software, music, movies, files, graphics, documents, messages, and other material.

Email – Electronic messages distributed by electronic means from one computer user to one or more recipients via the Internet and a distributed network.

PROCEDURES

Use of the Internet must be tempered with common sense and good judgment.

If employees must access the Internet for personal reasons, the activity should not interfere with job responsibilities or other employee's productivity.

When using Evidence Action computers and/or Internet connection, employees must not:

- Use Evidence Action's Internet connection to download or stream movies or video illegally, obtain music illegally, download games, entertainment software, or system modifications.
- Illegally copy material protected under copyright law or other licensing, or make that material available to others for copying. This includes software, music, movies, files, graphics, documents, messages, and other material you wish to download or copy.
- License or download any material for which a registration fee is charged without first obtaining the express written permission of your supervisor and/or the IT department.
- Download files from suspicious sources on the Internet, open email attachments from unrecognized senders, or use disks or thumb drives from non-Evidence Action sources.
- Introduce malicious software onto Evidence Action's network, and/or jeopardize the security of the company's electronic systems.
- Use Evidence Action systems to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

If an employee suspects that a virus, malware, or other malicious software has been introduced onto an Evidence Action computer, the employee must alert the IT department immediately. The employee should also immediately disconnect their computer from the local network (either by disconnecting the Ethernet cable, or disabling Wi-Fi), and shutdown the computer. These steps may prevent further damage or the propagation of the malicious software.

Employees may not access, send, receive, solicit, print, copy, or reply to confidential or proprietary information about Evidence Action, its employees, clients, suppliers, and other business associates without explicit permission. Employees should consult with their immediate supervisor for approval from the appropriate group responsible for permission to use or share information about Evidence Action (such as IT, External Relations, or HR).

Violations of this policy will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

FURTHER INFORMATION

For additional information, please contact the IT Department.

HISTORY

Origin: 16 August 2017
Last updated: 1 December 2021

Onboarding & Offboarding	**Policy Effective Date:** 1 November 2017
	Department of Origin: IT
	Policy Number: IT.GL.04

PURPOSE

The purpose of this policy is to describe the steps by which new employees are provisioned, trained, and assigned access for their functional duties within the company. Similarly, this policy describes the appropriate procedures for transitioning employees out of the company and/or role. The purpose of this policy is to create consistency around the addition and subtraction of employees from the company, and to streamline the execution of these tasks.

POLICY

Evidence Action is committed to supporting employees in their successful transition into and out of our workplace. The purpose of this is to allow sufficient time to complete supporting tasks for the employee change, such as provisioning accounts, purchasing computer equipment, preparing workspace, etc.

As an employee is onboarded, they will receive Company Equipment and be expected to participate in orientation activities for different functional areas, including IT. During this orientation process, they will be familiarized with the standard technologies used across Evidence Action as a whole, and any additional specific technologies that may be specific to their department or role.

Similarly, timely notice of an employee's departure or termination is required to ensure data ownership is maintained, prevent loss of proprietary data, and all confirm that Company Equipment is returned. A properly executed offboarding policy minimizes the risk surrounding employees departing the company, and the risk of proprietary data or knowledge being lost in the process.

DEFINITIONS

Onboarding – The action or process of integrating a new employee into a company and subsequently familiarizing them with internal practices.

Offboarding – The strategic process for transitioning employees out of a company and/or role.

Orientation – A component of onboarding that introduces a new hire to their new employment and environment. Orientation is a short-term activity or series of activities that typically takes place in the first week of employment.

Email – Electronic messages distributed by electronic means from one computer user to one or more recipients via the Internet and a distributed network.

Sensitive or Confidential Information – Such information may include records related to Human Resources, credit cards, donor records, social security numbers, program data & information, financial records & information, and more.

PROCEDURES

Onboarding

Hiring managers or HR are responsible for initiating the onboarding process as soon as a hire is made. All requests for employee onboarding should be sent to newhireadmin@evidenceaction.org to ensure all appropriate system administrators are properly informed. Requests made outside of this channel will not be fulfilled.

Upon onboarding, employees will be provided access to EA systems to commensurate with the responsibilities of their role.

Offboarding

The employee's supervisor and/or Human Resources should notify the IT department of employee offboarding, allowing sufficient notice to enable the securing of data, equipment, and other company assets prior to an employee's final exit.

All requests for employee offboarding should be sent to exit-admin@evidenceaction.org to ensure all appropriate system administrators are properly informed. Requests made outside of this channel will not be fulfilled.

At the time an employee offboards, the employee's supervisor and/or Human Resources should specify the details of closing the employee's accounts and provide details of data handling & access delegation. If the employee is the primary organizational owner of websites or other systems, the employee's supervisor should ensure those accounts are transferred accordingly with the support of the IT department.

Upon an employee's departure any equipment, laptop, computer, phone or other asset owned by Evidence Action will be immediately surrendered to their supervisor and/or the IT department. Evidence Action does not allow for equipment to remain in the possession of a departed employee. Evidence Action does not allow for equipment to be purchased by current or former employees for personal use.

In the event that Company equipment cannot be recovered cost-effectively and easily, the IT department will wipe all data remotely and restore the device to factory settings upon offboarding.

All employee accounts will be immediately disabeled once employment is complete. Access to Evidence Action systems will continue to be monitored to ensure there is no unauthorized access. All documents and files created for Evidence Action while employed at Evidence Action are solely the property of Evidence Action. Employees are prohibited from retaining any Evidence Action files or data after completion of their employment.

FURTHER INFORMATION

For additional information, please contact the IT department.

HISTORY

Origin: 16 August 2017
Last updated: 1 December 2021

Passwords and Authentication	**Policy Effective Date:** 1 November 2017
	Department of Origin: IT
	Policy Number: IT.GL.05

PURPOSE

This document provides the policy and guidelines surrounding the creation, use, and protection of Passwords and authentication methods for access to Evidence Action computers, systems and data. This policy applies to all Evidence Action employees. The purpose of this policy is to help ensure consistency in the use of Passwords and other authentication methods as the first line defense against unauthorized access to Evidence Action systems and data.

POLICY

Passwords, Single Sign On (SSO), and Multi-Factor Authentication (MFA) are the key features of Evidence Action's information and system security. They are the first line of protection for user accounts and organization data that may be accessed at any time from anywhere in the world. Access not secured with password and multifactor security, or configured to use SSO with Google accounts, may lead to the compromise of Evidence Action's data, systems, proprietary information, and operational functionality.

All systems must meet the following minimum organizational standards for access control:

- A password length of 8 or more characters;
- An annual password reset on the anniversary of last reset;
- Multi-factor authentication (MFA) configured.

If SSO configuration to Google Apps is available, access to systems should be configured accordingly. If SSO configuration to Google Apps is not possible, the minimum organizational standards above should be in effect.

DEFINITIONS

Multi-Factor Authentication – An extra layer of security that requires not only a Password and username but also something that only an individual user has on them; most commonly a mobile phone number that will receive a unique text code to verify the identity of the individual attempting to gain access.

Password – A secret string of characters (or phrase) that must be used to gain admission to a computer, interface, or system.

Password Management Software – An application that is used to store and manage the Passwords that a user has for various online accounts. Password Managers store the Passwords in an encrypted format and provide secure access to all the Password data with the help of a single master Password. One advantage of Password Managers is it enables the use of many highly complex (and difficult to remember) Passwords with the ease of a few clicks. Most Password Managers also assist in generating randomized complex passwords.

Access Control – A security technique that can be used to regulate who or what can view or use resources in a computing environment. There are two main types of access control: physical and logical. Physical access control limits access to buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

Authentication – The process of verifying the identity of a user or process attempting to access a computer, system, or data.

Sensitive or Confidential Information – Such information may include records related to Human Resources, credit cards, donor records, social security numbers, etc.

System Administrator – A person with the primary responsibility for the upkeep, configuration, and reliable operation of computer systems.

PROCEDURES

The following Password standards should be observed by all employees when accessing Evidence Action systems and Company Equipment:

- Passwords must be a minimum of 8 characters.
- Passwords must be changed every 365 days at minimum. Changed Passwords must be changed significantly and cannot repeat more frequently than every two years.
- Passwords should not be written down or stored electronically without encryption; if stored electronically, Password Management Software, such as the built-in Google Chrome capabilities, is recommended.
- Passwords must never be transmitted electronically in clear, plain text without appropriate encryption and obfuscation.

All users must access systems using their own user account and Password. All Passwords must be kept confidential and not shared. Any employee who suspects that their password or account has been compromised should immediately contact the IT department.

System Administrators are responsible for understanding and implementing the minimum organizational standards and should reach out to the IT department for assistance if needed. IT will collaborate with System Administrators to address any challenges to these requirements. Once SSO is configured for a system, no user should be exempted from SSO requirements without explicit approval by Global IT.

In the event that SSO cannot be supported by a system, or SSO only cannot be enforced for all users of a system, Global IT will assist System Administrators in configuring password and access controls for users. Global IT will provide explicit approval to any proposed exceptions to this policy.

Violations of this policy may result in disciplinary action up to and including discharge.

FURTHER INFORMATION

For additional information, please contact the IT Department.

HISTORY

Origin: 16 August 2017
Last updated: 1 December 2021

Bring Your Own Device (BYOD)	**Policy Effective Date:** 1 December 2021
	Department of Origin: IT
	Policy Number: IT.GL.06

PURPOSE

This policy defines standards, procedures, and restrictions on the usage of Personal Devices (including laptops, tablets and smartphones) for Evidence Action purposes. This policy applies to all Evidence Action employees who use Personal Devices to access Evidence Action data, systems, or resources. Use of Personal Devices for Evidence Action purposes constitutes consent by the user to all of the terms and conditions of this policy.

The purpose of this policy is to protect the integrity of Evidence Action's technology infrastructure, including external cloud services. This policy intends to prevent Company Data from being deliberately or inadvertently stored or accessed insecurely on a mobile device or carried over an unsecure network where it could potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the company's reputation. Therefore, all employees employing a Personal Device for Evidence Action purposes must adhere to this policy.

POLICY

All employees who wish to use Personal Devices for Evidence Action purposes must employ security measures deemed necessary by the IT Department. It is imperative that any Personal Device that is used to conduct Evidence Action business be used appropriately, responsibly, and ethically. Failure to do so may result in suspension or termination of access privileges so as to protect Evidence Action's technology infrastructure.

Use of Personal Devices to backup or store any Evidence Action-related information is strictly forbidden. Files, data, and other information are not to be downloaded to Personal Devices. If files, data, and other information are required to be downloaded to Personal Devices in exceptional circumstances, these should be deleted as soon as possible.

All users of Personal Devices to access Company Resources must employ reasonable physical security measures. Employees are expected to secure all such devices whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, screen lock, and physical control of such devices.

In the event of a data breach on a Personal Device used to access Company Resources, it is incumbent on the user to report the data breach to the IT Department.

In the event of a lost or stolen Personal Device that is used to access Company Resources, including email, it is incumbent on the user to report the incident to the IT Department immediately. Password resets will be required for the Evidence Action accounts accessed from the lost or stolen Personal Device.
In the event of a sale, disposal, or upgrade of a Personal Device, it is incumbent on the user to sign out of Evidence Action accounts accessed on the device before it is no longer in their possession.

The IT department reserves the right to refuse, by physical and non-physical means, the ability to connect Personal Devices to Company Resources. The IT department will engage in such action if such equipment is being used in a way that puts the company's systems, data, and users at risk.

Additional Requirements for High Risk Users
The following employees are deemed "high risk":

- Users who routinely access Confidential Data using Personal Devices;
- Users who frequently access Company Resources through unsecured networks while traveling;
- Users who have administrator-level access to sensitive systems ***and*** access these systems using their Personal Devices (e.g. ProcessMaker, Intacct, BambooHR, Salesforce, ADP TotalSource).

These employees are required to comply with the following additional requirements of this policy.

Endpoint Management Software
Evidence Action uses endpoint management software to secure mobile devices and enforce policies remotely. Before employees access Confidential Data or systems using Personal Devices, the endpoint management software client application must be installed and the device must be set to be manageable by the IT Department.

The endpoint management software enables the IT Department to take the following actions on mobile devices: remote support, remote wipe, location tracking, application visibility, and hardware feature management. Each capability will only be used as needed.

Any attempt to contravene or bypass the endpoint management software implementation will result in suspension of account privileges to Company Resources, and there may be additional consequences.

Security
Employees using Personal Devices to access Company Resources must use secure data management procedures. All Personal Devices must be protected by a strong password or PIN. Employees agree to never disclose their passwords to anyone if Company Resources are accessed on Personal Devices, and should utilize a separate Windows login if on a shared device.

Personal Devices must have appropriate security measures installed (e.g. up-to-date antivirus, anti-malware, firewall software and patch management) as deemed necessary by the IT Department.

Any Personal Device that is being used to access Company Resources must adhere to the authentication requirements found in IT.GL.05.

DEFINITIONS

Personal Device - Refers to a smartphone, tablet, laptop or computer owned by an individual.

Company Resources - Refers to all Evidence Action owned systems and services, such as Google Drive, Box, Intacct, BambooHR, etc. Also includes files and folders hosted on any such systems and services.

Company Equipment - any computer, laptop, mobile phone, tablet or other physical asset that is owned by Evidence Action, most commonly for the purpose of enabling employee work.

Antivirus - Software designed to detect and eliminate computer viruses

Firewall - A firewall is a network security device (software or hardware) that filters incoming and outgoing traffic to a device or computer network based on some set security rules.

Antimalware - Software designed to prevent, detect, and remediate malicious programming on individual computing devices and IT systems.

Endpoint Management Software - A tool enabling the unified administration of company or company computing equipment, including features such as hardware & software inventory, patch management, mobile device management, operating system and software deployments, and more.

Confidential Data - Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Please see GO.GL.1 for more detail.

FURTHER INFORMATION

For additional information, please contact the IT department.

HISTORY

Origin: 1 December 2021

System Data Backup, Recovery, and Continuity	**Policy Effective Date:** 1 December 2021
	Department of Origin: IT
	Policy Number: IT.GL.07

PURPOSE

This policy concerns the minimum requirements for an Evidence Action system in relation to the backup, recovery, and continuity of stored company data. The purpose of this policy is to ensure there are recovery options in the event company data or systems suffer corruption, loss, or modification either as a result of a disaster or other incident.

POLICY

Evidence Action's systems play important functions and contain critical information, and the interruption of systems could have major consequences. The ability to recover operations in such an event is therefore paramount. The IT department will partner with system administrators and owners to understand their system's backup and restoration options, and to perform periodic per-system assessments with an eye towards automation, cost efficiency, and suitability.

All systems at Evidence Action should have recovery planning in place, either as a service by the providers or configured internally in conjunction with the IT Department.

Systems should allow for the single instance or total recovery of lost or modified data for at least 14 days. Company data, files, version history, and a log of all changes to content should be recoverable for at least 14 days.

Each system should keep a log of all actions taken by administrators for at least one year. This log should be protected from editing by Evidence Action employees.

DEFINITIONS

Backup- An export or copy of data maintained separately from the production data in the system.

Recovery- The act of restoring data from a backup or other source to the production system.

Recovery Plan- A document containing the procedures, authority, and details of when and how data recovery will be authorized to take place.

Continuity- The ability to continue operating during an incident requiring data recovery with minimal downtown for users. Supported by a recovery plan.

Log- A journal automatically kept by systems of certain types of actions.

Service Provider- A company or entity who provides services, software, or other functionality in a contractually agreed upon manner.

PROCEDURES

The IT department will partner with system administrators to assess and review system backup functionality. This review will ensure that the backup features or tools planned or in place are functioning as the system operators understand, and meet the requirements of this policy, and any other legal or regulatory requirements. The IT department will provide annual assessments to system owners and administrators validating configured backup services and recommending improvements as needed. For new system acquisitions, the IT department will assess backup configurations during the selection process.

The IT department in conjunction with system administrators will determine if longer term recovery options are necessary. Recovery systems should maximize cost effectiveness and prioritize automation in their selection and setup.

FURTHER INFORMATION

For additional information, please contact the IT Department.

HISTORY

Origin: 30 June 2021

Domain Name Registration	**Policy Effective Date:** 1 October 2023
	Department of Origin: IT
	Policy Number: IT.GL.08

PURPOSE

This document provides the policy and procedures for the registration and usage of domain names to represent Evidence Action on the World Wide Web. The purpose of this policy is to define criteria for using and registering domain names and ensure the centralized management of domain names to maintain Evidence Action's identity.

Importance of evidenceaction.org Domain Name
Having a website with evidenceaction.org domain name enhances the credibility and legitimacy of Evidence Action compared to relying solely on social media platforms or using another entity's domain. The evidenceaction.org domain name provides a distinct identity and reinforces Evidence Action's presence on the internet.

Scope of the Policy
This policy applies to all new domain names registered after the effective date of this policy. It applies to domain names only and does not apply to web contents and where websites are hosted.

POLICY

Domain Name Registration
Evidence Action requires all domain names to be registered through reputable domain registrars such as GoDaddy, Network Solutions, AWS, Microsoft, Google, etc. This ensures reliability and adherence to industry standards. As Evidence Action continues to grow, it is necessary to:

- Centralize all domain names: All domain names associated with Evidence Action must be managed and controlled centrally to maintain consistent branding and control over web properties.
- Establish Evidence Action's identity: Registering domain names under the evidenceaction.org domain consolidates Evidence Action's online presence and strengthens its brand recognition.

Domain name registration requirements
It is recommended that Evidence Action web applications, websites, and any web presence utilize the evidenceaction.org domain name wherever possible. This can be achieved by requesting a subdomain from Evidence Action's Global IT team.

For instance, instead of registering a new domain name like 'apps.org,' use the domain name 'apps.evidenceaction.org.' In this example, 'apps' is a subdomain of the primary domain name evidenceaction.org. This approach ensures consistency, reinforces Evidence Action's identity, and eliminates the costs associated with registering new domain names.

Exceptions
In exceptional cases, there may arise situations where it is deemed necessary to register a new domain name. Such cases will be evaluated on a case-by-case basis.

DEFINITIONS

Domain Name - an online web address used to uniquely identify a website. Each website has its own unique domain name. For Evidence Action, the official domain name is www.evidenceaction.org.

PROCEDURES

To register a new domain name, a request must be submitted to the Global IT team at helpdesk@evidenceaction.org . If an exception is requested, proper justification should be provided. If denied, the request will be escalated to the COO for further consideration. This process ensures careful consideration and maintains the centralized control of domain names. All new domain names must be registered by Global IT.

By adhering to this Domain Name Registration Policy, Evidence Action ensures the centralized management of domain names, strengthens its online presence, and maintains consistency in branding across all web properties.

FURTHER INFORMATION

For additional information, please contact the IT Department.

HISTORY

Origin: 1 October 2023

Appendix A. Communications Systems in Use at Evidence Action

Communication Channel	Notes
Email (@evidenceaction.org or @eaiiadvisors.in)	Used by all employees, the company's official communication medium. Official business decisions, contracts, or correspondence with external parties should be conducted via email, this helps to ensure an enduring record exists and is discoverable in the future.
Slack	Used primarily for one-on-one chat by global employees and those who frequently communicate internally with other employees. Official business decisions should be made via email and not Slack, as Slack message history is not perpetual.
Google Meet	Used as the primary, everyday conferencing system throughout the organization.
Zoom	Used among a limited number of employees as a secondary conferencing system where advanced functionality is required (e.g. greater access control/security, advanced call administration, recording, etc.)
WhatsApp	To be used with caution, infrequently, and only for informal one-on-one or group chat. May be more convenient or efficient when working in remote areas or with limited connectivity. Official business decisions should be made via email and not WhatsApp, as WhatsApp accounts are not owned by Evidence Action and may not be secure.
Skype	To be used with caution, infrequently, and only for informal one-on-one or group chat or calls. May be more convenient or efficient when working in remote areas or with limited connectivity. Official business decisions should be made via email and not Skype, as Skype accounts are not owned by Evidence Action and may not be secure.