Student Name: Joy Muchangi

Acceptable Use Policy for Mbaririru Data Centre

Policy foundation

Purpose

Mbaririru Data Centre ("we" or "the company") Acceptable Use Policy will be used to ensure confidentiality, integrity and availability of Mbaririru Data Centre, data and the client assets. This policy will apply to employees, customers, visitors, vendors, interns and any personnel interacting with Mbaririru's hardware, network, software, and resources. By subscribing to the use of any of our resources, you are bound by this policy and failure to comply will result in the termination of the services and immediate suspension from the company resources and facilities until the issue is fully resolved.

Scope

The resources that are bound by this policy are both physical and onsite and are not limited to:

- Routers, Switches, Firewalls, Access points, Load balancers,
- Datacentre facility itself, security camera systems, HVAC systems, power infrastructure
- All operating systems including Linux distribution, Windows Server, hypervisors and the Operating systems on all the network devices.
- All the customer computers, laptops, mobile phones and any technological devices that are used to access the Mbaririru's network and to configure and manage the customer's environment.
- All management systems used on Mbaririru's infrastructure, customer applications that are hosted on the network and infrastructure as well as the internal email and communication software used.
- All the data that is hosted, stored or processed on Mbaririru Infrastructure.
- All the connections such as secure shell (SSH), Remote Desktop services (RDP), VPN and other related connections used to access the environment remotely.

Definition of key terms

Mbaririru infrastructure: All the resources as listed in the 'Scope' section of the policy.

User: Any personnel with authorized access to Mbaririru's Assets.

Client: Customer that is responsible for identifying and protecting the data that is hosted on Mbaririru Infrastructure.

Prohibited Use: Any action performed that is against this policy.

User Duties and Data Management

User responsibility

All users should follow the entry / exit security protocols and ensure they have visible Identifications on them once they are inside the Facility. Any user should be able to identify themselves by their government name and their association to Mbaririru upon request by the security personnel in charge.

All doors, racks accessed, and cages are to be closed upon entry. In places where there are security barricades, each person should go though security one at a time (no tailgating)

Ensure the account you use is explicitly assigned to you. There should not be any shared credentials, secret keys, public keys or Multi-Factor Authentication Tokens.

The accounts and roles created are to ensure least-privilege access and only when authorized should the access be increased.

All users are to ensure they replace the default password for all systems with their own username and passwords.

Users are to connect only to the asset-tagged and monitored devices. Any illegal access to devices such as access points, secure networks are prohibited.

Connecting to the infrastructure using personal and USB devices is prohibited unless approved explicitly and scanned by security.

Ensure screens are locked when unattended and maintain clean desks all through the facility.

No users are allowed to bring food or drinks of any nature inside the facility. All food items brought should be left in the safe boxes provided at the security gate.

Users are to report any found/missing devices, badges to the security personnel in charge.

Users will ensure they use the recommender routes to access the building and only use the emergency routes in the case of an emergency or when need arises.

Users are to ensure their data adhere to the set legal requirements such as HIPAA/ PCIDSS/GDPR as applicable.

Ensure all the software used on the Mbaririru's infrastructure is licensed and have no corrupt or pirated versions.

Data Protection and handling

This applies to all the data whether stored, accessed, transmitted or processed within the Data Centre and any connected environments.

Least privilege, classification, transmission

All data is to be classified before it is stored or transferred.

All sensitive data held should have more access control measures such as regular reviews and audits and biometric scanners.

All data is to be encrypted both at rest and in transit.

Users are to ensure they enforce least privilege access and use role-based access control for critical actions.

Data should be transferred only by authorized and approved third party vendors.

Prohibited Use and Violations

Prohibited Activities

Systems security means the personnel designated to ensure and manage security policy and infrastructure.

Any form of system modification such as performing OS installations, uninstalling system software, deletion or changing of system and configuration files without written approval from the System security team.

Any actions performed suspected to bypass the systems security such as disabling logging software, altering with the firewalls, rerouting network traffic, tampering with video monitoring systems and alarm systems.

Usage of applications such a Nmap, netstat and any network port scanning software against Mbaririru’s systems without authorized permission.

Spam Mail and Hacking

Usage of botnets to distribute and host and execute malware and worms, be it in client’s virtual space or Mbaririru’s infrastructure is prohibited.

Sending of spam email as promotional material that is not connected to the business purpose.

Performing actions such as Brute-force, password spraying, phishing, smishing or any attempt to exploit systems and software vulnerabilities.

Any research that is performed on Mbaririru’s security infrastructure without formal written authorization will be considered as Unethical hacking.

Obscene Material and Child pornography

CSAM – Child Sexual Abuse Material is the term that will be used in place of “child pornography” to ensure emphasis on the criminal nature of the content.

Trafficking means organizing and sourcing people for cheap labour or commercial sex. It can be creating advertisements or managing data for people illegally.

All material that is sexually explicit and in other nature inappropriate should not be stored, created, viewed or distributed on any accounts or software in Mbaririru’s infrastructure.

Hosting, creating, managing social media pages, promoting of sexually explicit services such as subscribing to platforms as OnlyFans, using Mbaririru’s infrastructure is prohibited.

Any CSAM material found on the client’s software or having been installed on Mbaririru’s infrastructure by a client, will not be tolerated and if found, will lead to immediate termination and closure of accounts and access to the Datacenter both physically and remotely.

Mbaririru has the authority to contact National law-enforcement and the necessary organizations involved with keeping the law and ensuring order and will submit necessary information in observance to legal and privacy obligation.

Using Mbaririru’s infrastructure to organize and facilitate adverts, payments, and meetings in favour of trafficking.

Enforcement and Governance

Privacy and monitoring

By agreeing to use Mbaririru’s infrastructure, you are giving consent to the recording, auditing, collecting, screening of the data transferred, stored and viewed on Mbaririru’s Systems. This will only be done by certified and authorized personnel working with us.

Any data that is on Mbaririru’s infrastructure will not be private and can be accessed and disclosed in case of any incidents, operational requests, or incident response purposes.

Mbaririru has the permission to monitor but not limited to network traffic, file access, administrative interfaces and emails and messaging content.

Complaints procedures

In case of any suspected broken policy, each is supposed to report immediately and in a confidential manner to this hotline +1-021-111-021, or email [reports@mbaririru.com].

All general queries should be addressed to [queries@mbaririru.com].

To ensure all evidence is not tampered with we ask that after reporting the issue, kindly speak to the Security Team in charge and they will decide on how to move forward.

Discipline Framework

In the event of a violation to the Mbaririru Data Centre AUP, the following disciplinary steps will be taken, and each action will be recorder by the management team.

Level 1: Initial Warning

Each client will receive a formally written letter that will indicate the reasoning for the discipline action and include the right actions required.

Level 2: Second Warning

In the event, multiple Level 1 notices have been sent, the client is issued with a second warning which, is already sent, the issue will be escalated to Level 3.

Level 3: Limitation of access

Access to Mbaririru's Infrastructure will be suspended for a defined period of time by the compliance team until a review is done and the client cleared.

Level 4: Termination of contract/ access

The client access and contract will be immediately terminated and if need be reported to the necessary legal government authorities.

Zero-tolerance offences:

All actions indicated under this will have Level 4 enforced immediately.

Child Sexual Abuse Material: Actions done in favour to CSAM

Illegal Activities: All actions that are depicted as serious crimes and felony under applicable law.

Violent threats: Any evident threats of harm, terrorism and violence against Mbaririru Data Centre as well as the infrastructure and its employees.

Policy revision and acknowledgement

This policy will be reviewed Annually in October by Mbaririru Legal Compliance team and any changes made will be communicated through official channels (Email, Websites, announcements.

Clients are to revise the policy at the renewal of their contract which will happen on an annual basis and in the case of any revision made to the policy.