Maluki Muthusi P15/81741/2017

0.1 The Company

Security policy document for Tuzo Kenya Limited (TKL). TKL is a Kenyan SME that deals with buying and processing milk from Kenya farmers. It has various departments that handle specific tasks including, getting the raw product from farmers, processing it, storing, marketting, selling, paying farmers, educating farmers and running other community help programs.

Introduction

A security policy for an organization explains each employee's responsibilities for protecting systems and data within the organization. A security policy is a set of standardized practices and procedures designed to protect a business's network from threat activity. Typically, the first part of the cybersecurity policy is focused on the general security expectations, roles, and responsibilities within the organization. The second part may include sections for several areas of cybersecurity, such as guidelines for antivirus software or the use of cloud applications. Policies should always prioritize the areas of importance to the organization, such as including security for the most sensitive and regulated data.

Acceptable use policy (AUP)

An AUP is used to specify the restrictions and practices that an employee using organizational IT assets must agree to in order to access the corporate network or systems. It is a standard onboarding policy for new employees, ensuring that they have read and signed the AUP before being granted a network ID. (Institute 2014*a*)

No	Policy	Justification
1	TKL proprietary information stored on electronic and computing devices whether owned or leased by TKL, the employee or a third party, remains the sole property of TKL. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.	Every employee should understand the company owns the electronic devices and its information.

2	You have a responsibility to promptly report the theft, loss or unauthorized disclosure of TKL proprietary information.	It is crime for an employee to steal from the company or to witness and fail to report.
3	You may access, use or share TKL proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.	Employees are not allowed to missuse company resources doing operations that are not work related.
4	Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems.	Departments can create rules regarding how employees can access the internet or the internal network. For example the infrastructure department may block internet access from the internal machines.
5	For security and network maintenance purposes, authorized individuals within TLK may monitor equipment, systems and network traffic at any time.	Employees should be aware that when using the company's network, traffic may be monitored for security purpose.
6	All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.	The company has put restrictions such as, older browser versions are not allowed.
7	System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.	Employees are advised to use strong authentication mechanisms over weak ones. They are advised to opt in to multifactor authentication.
8	All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.	Employees should not leave a device unlocked for a long time

9	Postings by employees from a TKL email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of TKL, unless posting is in the course of business duties.	Employees should put this in their social media, e.g Twitter, Facebook. This will help people from misinterpretting them.
10	Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.	Employee should be aware of phishing schemes.
11	Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).	It is a crime to introduce viruses to the TKL computers.
12	Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).	It is a crime to block other employees from accessing the companies services.

Data breach response policy

The goal of the data breach response policy is to describe the process of handling an incident and remediating the impact on business operations and customers. This policy typically defines staff roles and responsibilities in handling an incident, standards and metrics, incident reporting, remediation efforts, and feedback mechanisms. (Institute 2016)

Disaster recovery plan

A disaster recovery plan is developed as part of the larger business continuity plan, which includes both cybersecurity and IT teams' recommendations. (Institute 2014*b*)

Business continuity plan

A business continuity plan (BCP) describes how the organization will operate in an emergency and coordinates efforts across the organization. Additionally, BCP will work in conjunction with the disaster recovery plan to restore hardware, applications, and data that are considered essential for business continuity.

Remote access policy

Organizations can implement a remote access policy that outlines and defines procedures to remotely access the organization's internal networks.

Access control policy

An access control policy (ACP) defines the standards for user access, network access controls, and system software controls. Additional supplementary items often include techniques for monitoring how systems are accessed and used, how access is removed when an employee leaves the organization, and how unattended workstations should be secured.

References

Institute, S. (2014*a*), 'Consensus policy resource community'.

Institute, S. (2014*b*), 'Disaster recovery plan policy', https://assets.contentstack.io.

Institute, S. (2016), 'Data breach response policy', https://assets.contentstack.io.