ICT Security Policy for ABC Supermarkets

# Internet

This Internet Usage Policy applies to all employees of ABC Supermarkets who have access to computers and the Internet to be used in the performance of their work. Use of the Internet by employees of ABC Supermarkets is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the Internet through ABC Supermarkets is a privilege and all employees given this access must adhere to the policies concerning its usage. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment. Employees may also be held personally liable for damages caused by any violations of this policy. All employees are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder.

## Access

* Access to the internet will be provided on a “need to use” basis. Only employees who require access to the internet to execute their duties will be provided such via a company issued device.
* Web sites will be filtered for malicious intent and users will be blocked from accessing any sites that are flagged as dangerous. If any websites needed by users in the completion of their duties are inadvertently flagged and blocked, a report to the ICT department must be made and the site will be unblocked once found to be none threating.
* Hacking into any unauthorized networks and systems, both internal and external, using the company’s resources is prohibited.
* All Internet data that is created, transmitted and/or received by ABC Supermarkets’ computer systems is considered to belong to ABC Supermarkets and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

# Internal Network

The purpose of this policy is to define the standards for connecting computers, servers, mobile or other devices to the ABC Supermarkets’ network. These standards are designed to protect the network and the ability of employees of ABC Supermarkets to use it. They serve to advance the productivity of the company while also minimizing damage that could result from networked devices that are not configured or maintained properly and to ensure that devices on the network are not taking actions that could adversely affect network performance or the reputation of the company.

* Internal network access will be provided on a “need to use” basis.
* The internal network will be segmented into work groups (e.g. Marketing, Inventory, Accounts, etc.). Employees issued with company devices will be given access to only the workgroups required for them to execute their duties.
* Wireless access will be granted only to laptops and other needed devices.
* Access will be filtered by MAC addresses to ensure that only authorized devices can gain access to the core network.
* Any provided networks for guest and employees to use along with their own devices will be physically separated from the internal network to prevent any infiltration from the publicly opened network.

# EPOS (Electronic Point of Sale)

The EPOS system is used by ABC Supermarkets to monitor, control stock, perform sales analysis, collect data on customers with loyalty cards and help analyze customer spending habits. The system comprises of a printer, magnetic card reader, laser scanner, scale, cash drawer, display, EPOS processor and a central server for storing product information.

* The EPOS system will be given access to the internet only if required for system updating/upgrading purposes.
* The EPOS will be separated onto its own network segment with restricted access via the Inventory and Accounting departments personnel.
* Access to the system will be time restricted to prevent any unauthorized entry outside of normal working hours.
* Remote access will be restricted to specific IP addresses.
* Authorized users will be required to login using their fingerprints. This is to remove any possibility of a lost or stolen password being used to gain entry to the EPOS system.

# Physical Access

Access to the warehouse, accounting office and administration office spaces will require employees to use a magnetic access card, with their picture printed, when gaining access. The cards will be programmed with time limits and department access restrictions on a “need to use” basis.

* Strong username and password will be employed to give authorized users access to the computer systems. Users will be required to change their password every 60 days.
* Antivirus software will be configured to run daily scans.
* Hard drives will be encrypted, and keys stored securely in a central location
* USB access will be restricted.
* Instillation of software will be restricted.

# New Recommended Solutions

## Firewall:

New firewalls can be equipped with both IDS (Intrusion Detection Software) and/or IPS (Intrusion Prevention Software) to help prevent and identify any threats that may come against the network or gained entry to the network. FortiGate 100F firewall uses IPS technology to hep secure the network. This device is among the Next Generation Firewall systems designed for today’s cyberthreats.

## Antivirus

I would recommend using a centrally managed antivirus solution to monitor and keep individual computers secure. Sophos Endpoint Protection is a solution that scores high when compared to other solutions. It has anti-ransomware and artificial Intelligence among its protection tools and can be managed from a central location.