# Optimum Commercial Solutions t/a Optimum ELITE

Optimum ELITE
Protection, not restriction

## Information Security Policy

### 1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it to all employees and contracts as applicable.

### 2. Information Security Policy

Optimum Commercial Solutions Ltd t/a Optimum ELITE and its appointed representatives handles sensitive customer information. Sensitive Information must have adequate safeguards in place to protect them, to protect customer privacy, to ensure compliance with various regulations and to guard the future of the organisation.
Optimum Commercial Solutions Ltd t/a Optimum ELITE commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process customer information so that we can meet these promises.

Employees handling Sensitive customer data should ensure that they:
• Handle Company and customer information in a manner that fits with their sensitivity;
• Limit personal use of Optimum Commercial Solutions Ltd t/a Optimum ELITE information and telecommunication systems and ensure it doesn't interfere with their job performance;
• Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
• Do not disclose personal information unless authorised;
• Protect sensitive customer information;
• Keep passwords and accounts secure;
• Request approval from the network/management prior to establishing any new software or hardware, third party connections, etc.;
• Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
• Always leave desks clear of sensitive customer data and lock computer screens when unattended;
• Information security incidents must be reported, without delay, to the individual responsible for incident response locally.

Optimum Commercial Solutions Ltd t/a Optimum ELITE reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from Optimum Commercial Solutions Ltd t/a Optimum ELITE.

## 3. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Optimum Commercial Solutions Ltd t/a Optimum ELITE established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorised access to confidential data which includes customer data.
- Employees should ensure that technologies should be used and setup in acceptable network locations.
- Keep passwords secure and do not share accounts.
- Authorised users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password protected screensaver.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Company email address to social media should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Optimum Commercial Solutions Ltd t/a Optimum ELITE unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

## 4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of contract/employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

## 5. Protect Stored Data

All sensitive customer data stored and handled by Optimum Commercial Solutions Ltd t/a Optimum ELITE and its employees/appointed representatives must be securely protected against unauthorised use at all times. Any sensitive customer data that is no longer required by Optimum Commercial Solutions Ltd t/a Optimum ELITE and its appointed representatives for business reasons must be discarded in a secure and irrecoverable manner.

## 6. Information Classification

Files and media containing data must always be labelled to indicate sensitivity level.

• Confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Optimum Commercial Solutions Ltd t/a Optimum ELITE if disclosed or modified.

• Internal Use data might include information that the data owner feels should be protected to prevent unauthorised disclosure;

• Public data is information that may be freely disseminated.

## 7. Access to the Sensitive Customer Data

All Access to sensitive customer data should be controlled and authorised. Any Job functions that require access to customer data should be clearly defined.

• Access rights to privileged user IDs should be restricted to the least privileges necessary to perform job responsibilities.

• Privileges should be assigned to individuals based on job classification and function (Role based access control).

• Access to sensitive customer information such as personal information and business data is restricted to employees that have a legitimate need to view such information.

• No other employees should have access to this confidential data unless they have a genuine business need.

• When customer data is shared with a Service Provider (3rd party) this must be documented within Optimum Commercial Solutions Ltd t/a Optimum ELITE's CRM system.

• Where 3rd Party Service Providers are registered with Optimum Commercial Solutions Ltd t/a Optimum ELITE, we will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the customer data that the Service Provider possess.

• Where 3rd Party Service Providers are not registered with Optimum Commercial Solutions Ltd t/a Optimum ELITE, employees/appointed representatives must ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the customer data that the Service Provider possess.

## 8. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

• Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

• Employees should ensure that they are authenticated for the use of technologies.

• Employees should take all necessary steps to prevent unauthorised access to confidential data which includes card holder data.

• Employees should ensure that technologies should be used and setup in acceptable network locations.

•A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.

• Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts.

•Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
• Media containing sensitive customer information must be handled and distributed in a secure manner by trusted individuals.
• Visitors must always be escorted by a trusted employee when in areas that hold sensitive customer information.
• Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where customer data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on Optimum Commercial Solutions Ltd t/a Optimum ELITE & appointed representative’s sites. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
• Strict control is maintained over the external or internal distribution of any media containing customer data and has to be approved by management.
• Strict control is maintained over the storage and accessibility of media.
• All computers that store sensitive customer data must have a password protected screensaver enabled to prevent unauthorised use.

## 9. Disposal of Stored Data

• All data must be securely disposed of when no longer required by Optimum Commercial Solutions Ltd t/a Optimum ELITE or appointed representatives, regardless of the media or application type on which it is stored.
• All hard copies of customer data must be manually destroyed as when no longer required for valid and justified business reasons.
• Optimum Commercial Solutions Ltd t/a Optimum ELITE & appointed representatives will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
• All customer data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using secure deletion processes or the physical destruction of the media;
• If secure wipe programs are used, they must define the industry accepted standards followed for secure deletion.
• All customer information awaiting destruction must be held in lockable storage containers clearly distinguishable from information to be retained - access to these containers must be restricted.

## 10. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees.
• Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day company practice.
• Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document.

• All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the Company.
• Company security policies must be reviewed annually and updated as needed.

## 11. Network Security

• Optimum Commercial Solutions Ltd t/a Optimum ELITE will have firewalls between any wireless networks and the customer data environment.
• The firewall rules will be reviewed on a six months basis to ensure validity.
Source IP Destination IP Act

## 12. System and Password Policy

All users with access to Optimum Commercial Solutions Ltd t/a Optimum ELITE systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.
• System configurations must include common security parameter settings.
• The systems configuration standard should be applied to any news systems configured.
• Security parameter settings must be set appropriately on System components.
• All user must use a password to access the company network or any other electronic resources.
• All user ID's for terminated users must be deactivated or removed immediately.
• All system and user level passwords on Optimum Commercial Solutions Ltd t/a Optimum ELITE systems must be changed on at least a monthly basis.
• A unique password must be setup for new users and the users prompted to change the password on first login.
• System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands.
• Administrator access to web-based management interfaces is encrypted using strong cryptography.
• The responsibility of selecting a password that is hard to guess generally falls to users A strong password:
a) Be as long as possible (never shorter than 6 characters).
b) Include mixed-case letters, if possible.
c) Include digits and punctuation marks, if possible.
d) Not be based on any personal information.
• If an operating system without security features is used (such as DOS, Windows or MacOS), then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending program.
• To protect against network analysis attacks, both the workstation and server should be cryptographically secured.
• Two-factor authentication is implemented into Optimum Commercial Solutions Ltd t/a Optimum ELITE systems. This must be set up by users on a separate device prior to initial system login.

## 13. Anti-virus Policy

Optimum Commercial Solutions Ltd t/a Optimum ELITE is responsible for ensuring suitable anti-virus software is implemented into its systems. Appointed representatives are responsible for ensuring suitable anti-virus is implemented into their systems.

## 14. Patch Management Policy

• All Workstations, servers, software, system components etc. owned by Optimum Commercial Solutions Ltd t/a Optimum ELITE must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
• Wherever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors.
• Security patches have to be installed within one month of release from the respective vendor and have to follow the process in accordance with change control process.

## 15. Remote Access Policy

• It is the responsibility of Optimum Commercial Solutions Ltd t/a Optimum ELITE employees, Appointed Representatives and any relevant third parties with remote access privileges to Optimum Commercial Solutions Ltd t/a Optimum ELITE systems to ensure that their remote access connection is given the same consideration as the user's on-site connection to Optimum Commercial Solutions Ltd t/a Optimum ELITE.
• Secure remote access must be strictly controlled. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.
• 3rd party accounts with access to Optimum Commercial Solutions Ltd t/a Optimum ELITE systems network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.
• All hosts that are connected to Optimum Commercial Solutions Ltd t/a Optimum ELITE systems internal networks via remote access technologies will be monitored on a regular basis.
• All remote access accounts used by vendors or 3rd parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification.
• 3rd party accounts with access to Optimum Commercial Solutions Ltd t/a Optimum ELITE systems network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.