Cyber Security Policy

GENERAL

This document contains the general rules and procedures pertaining to the information security of Zenergy Connect cyber administrative information system (AIS); and the processing and exchanging of sensitive information. These rules and procedures are intended to support the goals and principles outlined in the standards described and/or desired within Cyber Essentials Plus.

It is intended to reflect, comply and be in accordance with the current Cyber Security Policies form the framework of the systems:

- ensuring confidentiality of information through the application of approved restrictions on access and disclosure of information;
- ensuring the integrity of the information by protecting against unauthorised access, alteration, or destruction of information;
- ensuring accessibility of information by ensuring reliable and timely access to information;
- ensuring information accountability by introducing control over access and rights over information resources.

1. Human resources security policy

1.1. Before the start of employment or 'on boarding' by Zenergy Connect

Before the start of employment, it is essential to ensure that employees or contractors understand their responsibilities and are fit to perform their assigned roles, to reduce the risk of theft, irregularities or other malicious activity with Zenergy Connect assets including its IT network.

1.2. Roles and responsibilities

The roles and responsibilities regarding information security of Zenergy Connect employees are spelled out in their employment contracts and job descriptions, as well as in the various regulations and guidelines that employees are required to familiarise themselves with and agree to comply with prior to and/or as a mandatory condition for their employment.

Before starting employment or contractual relationships, each party familiarises itself with the requirements through Zenergy Connect 'on boarding' process including the initial induction procedures outlined in the HR Manual and set out in ISO 9001 policies and procedures.

The effectiveness of the process is measured by the ratio of the contracts (job descriptions, annexes to contracts, etc.) that describe the roles and responsibilities of the parties in relation to information security to the total number of contracts.

1.2.1. Preliminary survey

Once Employees are appointed checks that are made are the following:

- For natural persons – search on the Internet with a view to establishing reputational risk; requirement of biography, diplomas, certificates before appointment or conclusion of a civil contract by decision of the Management;
- For legal entities – check on the Internet with a view to establishing reputational risk, check in the Commercial Register for recorded circumstances.

1.2.2. Conditions for starting employment or contract

As part of the package of documents, which every person (natural or legal) must sign, is the express written consent to comply with and comply with the rules and instructions of the organisation, part of which rules are the requirements for information security.

The effectiveness of this process is measured in the manner described in "Roles and Responsibilities" of this PS.

1.3. During the performance of employment or contract

The aim is to ensure that employees or contractual parties are familiar with information security issues, their responsibilities and obligations and have the necessary information and knowledge to fulfil information security requirements during the performance of their duties, as well as to reduce the risk of human error.

1.4. Responsibilities of management

Management requires all parties with whom it maintains contractual relationships, during their work, to comply in all aspects with information security requirements, as well as with all internal rules and guidelines, procedures, policies, etc., as well as with this document in particular. Before starting employment or contractual relationships, each party familiarises itself with the requirements of SUSI, which it certifies with a signature.

The effectiveness of this process is measured by the number of signatures certifying familiarity with the requirements of SUSI to the total number of persons subject to employment or other contractual relationships with the organisation.

1.5. Acquaintance with information security requirements, policies, and training

Every employee is instructed (trained) on the topic of cyber security upon starting work, and then once a year. The successful completion of the briefing is certified by the employee's signature.

2. Disciplinary Actions

Violation of cyber security by employees is considered a disciplinary offense and is treated and punished as such in accordance with Employment legislation and their contract of employment.

Violation of information security by persons who are not employees of the organisation is punishable according to contractual agreements. If necessary, the relevant authorities are contacted.

The effectiveness of this process is measured by the total number of violations and the total number of sanctions applied.

3. Termination or change of employment or contract

The purpose is to ensure that individuals (natural and legal) change or terminate their relationship with Zenergy Connect in the proper manner.

4. Responsibilities upon termination of employment

GL Telecom’s internal procedures define how to proceed when changing or terminating an employees' employment relationships.

Termination of contractual relationships (civil contracts, contracts with legal entities, etc.) takes place according to the clauses of the relevant contract.

Each person, upon termination of the person’s legal relations with the organisation, has the obligation to return to an acceptable state their assets assigned to them.

Any person upon termination of their legal relationship with Zenergy Connect immediately loses the right to use and/or access any information resources of the organisation.

The effectiveness of this process is measured by the ratio between correctly terminated/changed relationships to the total number of persons with whom relationships were terminated/changed for a given period.

4.1. Issue (return) of assets

Assets are issued and centrally logged in a central asset log to identify the user and what assets they have.

In case of refusal to return assets or in case of return of assets in an unsatisfactory condition, the organisation may action according to the situation.

4.2. Termination of access rights

Access rights to the premises are regulated by the organised throughput of the office, from the entrance door to the individual premises. Access rights to information resources are regulated by Zenergy Connect' systems administrator.

Upon notice of termination/change in relationships, the user rights to work with and otherwise access the systems are immediately terminated or immediately changed to reflect the change in role.

5. Physical security policy

Physical security includes a system of organisation, physical and technical measures to prevent unauthorised access to equipment and IT facilities. The system of measures includes the protection of the premises and facilities in which sensitive information is created, processed, and stored and the control of access to them.

5.1. Control of the physical integrity of computer facilities

All computer and software tools in the organisation must be provided with the minimum necessary means of protection (software, hardware and physical) corresponding.

IT hardware such as computers, or other IT equipment, should only be accessible in the presence of authorised employees.

6. Access Control Policy

This policy defines the access control requirements for the various systems used.

For the purposes of this policy, "system" means the network environment, servers, workstations, laptops, mobile phones operating systems, applications, terminals, other portable communication devices, and any devices used to store, process or exchange information within Zenergy Connect.

The scope of this policy includes all employees, Direct Labour, contractors, and any other who have access to the information resources of the Organisation.

Access to all systems must be controlled and refer to business requirements. Users must be explicitly granted access to systems or information.

Users receive permission to access applications or DB (database) from the Administrator after a written assignment from the management. Owners of information should approve or deny requested access based on the "need to know" principle and the requirements

of the position held and depending on the classification level of the data. When making a decision, the imposed legal restrictions, as well as contractual ones, must be considered.

6.1. Manage user accounts/passwords

Any type of access to systems containing sensitive information is controlled by an authentication method that includes the minimum combination of username (ID) and password.

For all systems, the administrator must:

- create a strong initial password: according to internal computer usage rules environment (See ZC's password creation policy). The password must be communicated personally to the user.
- whenever the system allows it, Zenergy Connect require passwords to be changed over time to meet this policy and ensure that the use of "trivial" passwords is prevented. Trivial passwords are those passwords that can be easily associated with the organisation or the employee – product names, locations, the employee, address, pet names, hobbies, birthday etc.
- prevent the use of trivial IDs: such as "Guest," "Temp" etc, unless specifically intended for a specific user and/or documented. Group or shared IDs should only be provided if they have a documented owner – a person responsible for all changes made by the account in question.

Where technically possible, systems should not allow users to access systems from multiple locations simultaneously.

Passwords are never to be stored in plain sight or written down on paper. Passwords are not to be saved by autofill forms.

6.2. User registration

All IS users must be provided with unique IDs Unique IDs must not be reused even after termination of employment with the employee.

Owners of the information are responsible for ensuring that user access is granted in accordance with business need, adheres to the "need to know" principle, and is removed as soon as it is no longer needed.

User registration and de-registration procedures must be documented and followed when access to all systems is changed. These procedures should include (but not be limited to) the following steps:

- obtaining approval from the owners of the information resources;
- confirming whether the given access is equivalent to approvals;
- maintaining registration logs to track who requested, approved, granted, verified, modified, or revoked access.

Use of another's account is strictly prohibited unless permitted by prior written permission.

6.3. Termination of access

Management is responsible for promptly notifying the lead HR and Administrator of changes in employee status to ensure immediate termination/change in access to the systems.

It is management's responsibility to ensure that all information assets provided to employees, such as laptops, workstations, badges, keys, access cards, tokens, software, data, documentation, manuals, etc., are surrendered upon termination of labour relations.

6.4. Periodic review of access rights to employee systems

System access rights (including those of administrators, super-users, and any other type of special users) should be reviewed at least once a year and always when an employee leaves.

User accounts that are not in use are to be locked and disabled.

6.5. Control access to operating system(s)

All users must have a unique ID. Use of personal, or group accounts must be approved in advance by the Administrator. Each such account must have a documented owner who is responsible for all actions performed by the account.

Such restrictions should be imposed so that no access is granted to anyone who is granted by default. Command-line access to server operating systems should only be allowed to system administrators responsible for maintaining the servers.

Unlocking an account and generating a new password can be done by the authorised persons only after confirming the identity of the employee.

During the process of logging into the system, a message should appear to the user, warning him that:

The system should be designed so that it does not provide any information on a failed access attempt about which part is wrong, ID or password and the number of attempts left before the account is locked.

Workstations and servers must be configured to lock user sessions after a certain period of inactivity. To unlock, it is necessary to enter the user password. The usual idle time is 10 minutes. Users should not attempt in any way to disable this control.

6.6. Application access control

All access to the Applications must be controlled by an authentication method involving a combination of username (ID) and password.

All users should be given minimal access sufficient to perform their duties. This can be achieved by using the following controls individually or in combination:

- logical conditions laid down within the application;
- limiting the availability of the application to authorised users only;
- limiting access to command line (command line);
- limiting application content and functionality based on user privileges and groups;
- restriction of authority: e.g. read-only access;
- where possible, access should be organised based on role and/or position, duties, and functions.

If the user is inactive for a maximum of 30 minutes, the session should be automatically terminated.

7. Policy for organising work with passwords

This policy regulates technical measures to ensure the processes of generating, changing, and terminating passwords, as well as the way of conducting control of officials when working with passwords.

1. GL Telecoms ensures that the processes of generating, changing, and terminating passwords in the AIS are conducted by the Systems Administrator.
2. Passwords for the company's IT subsystems are generated and distributed centrally based on the following rules:

a. the password is at least eight characters long, mixing upper- and lower-case letters, numbers and special characters;
b. when setting a new password, it must be different from the previous one;
c. the passwords for individual resources are different.
d. not to choose a password that is linked to the end user's personal data (name, date of birth, children, etc.)
e. not to write down passwords in a visible place (keyboard, monitor, desk, etc.).

3. When setting personal passwords, users bear personal responsibility for their compliance with the specified rules. When the generation of passwords is performed centrally – responsibility for their compliance lies with the Systems Administrator or another official to whom such duties are assigned.
4. The system for centralised generation, distribution and management of passwords must ensure officials have access only to their passwords.
5. Access passwords are changed on a scheduled basis, no less often than once every 180 days, unless for other security reasons such a change should be made more frequently.
6. Access passwords are changed on an extraordinary (unscheduled) basis in the following cases:
    a. compromising password(s);
    b. change in resource access rights without termination of access;
    c. complete reinstallation (reconfiguration) of hardware and software which are essential for certain subsystems;
    d. upon termination or change of rights (including upon dismissal) of an official whose functional duties were related to the centralised management of the password protection system in the IS;

7. In emergency situations or in the absence of a Systems administrator, the change/use of passwords is administered by a pre-determined deputy. Upon completion of the emergency response activities, the holder's password must be changed. Access to resources (username, passwords, etc.) are to be blocked immediately in the following cases in the absence of an official for a long time or dismissal;

8. Password-based access blocking is done automatically by the system. Resumption of access to a resource after establishing the reasons can only be done by the administrator.

9. Control of officials when working with passwords, compliance with the order for their replacement, storage and use is carried out by an administrator of means of protection with passwords (if one is appointed), the administrator and by the units and structures responsible for information security in the IS.

8. Internet use policy

The purpose of this policy is to indicate the permissible and impermissible types of use of Internet resources, including the use of browsers, personal mail, electronic real-time messaging (chat), uploading and downloading of files and voice communication in the office and its subsidiaries.

The Internet Acceptable Use Policy applies to all employees, contractors, subcontractors, vendors, visitors, and anyone using the IT assets of **Zenergy Connect** (for short "authorised users") who use any of the Internet resources of **Zenergy Connect.**

Basic principles Authorised users are allowed to use the Internet for business purposes.

All authorised users who have the right to use the Internet must comply with the following principles:

- Any use of the Internet that may be associated with the **Zenergy Connect** domain address (such as posting information in newsgroups, using chat programs and participating in mailing lists) must not discredit the organisation or associate it with controversial causes (e.g. materials with overt sexual content, defamatory statements, hate propaganda, etc.);
- Use of personal email to share work email is not permitted;
- Use of the Internet that could have a negative effect on **Zenergy Connect** is not allowed (such as playing resource-intensive games, audio and video streaming, chats etc.);
- Use of the Internet that could infringe copyright, trademarks, or patents (such as illegal downloading of music or movies) is not permitted;

- All authorised users are required to immediately notify the administrator of any suspicious use of company network assets or systems by submitting a General Incident request to the **Zenergy Connect** system administrator.

9. Email acceptable use policy

Users should draft emails and other electronic communications (WhatsApp, texts etc) as accurately, carefully, and correctly as they create any other written communication. Users need to be aware that any written electronic form of communication is accepted as evidence when legal relationships of any type arise.

Users must not use email for the following activities:

- send and forward chain letters;
- send and forward messages related to GL Telecom's cyber security, the origin of which is not from the Information Technology units of the organisation. (example: computer viruses, computer worms, etc.)

All email system settings that can be used to automatically forward a received message to another email address are accepted as Auto forward Rules.

The use of manual or automatic forwarding to forward **Zenergy Connect** business communications outside of it is not permitted.

In the event that an electronic message containing classified information is received in error, the recipient must notify the sender of the message and delete it.

The User must immediately notify the management of **Zenergy Connect.** upon receiving a message containing illegal or anti-competitive business information, or information that violates company procedures and policies.

10. Anti-malware security policy

This policy sets out **Zenergy Connect**'s IT protection policy against computer viruses entering its network.

1. Only licensed anti-virus software is allowed to be used by Zenergy Connect. The current anti-virus system used is WatchGuard EPDR and is reviewed annually to verify it represents at least industry standard anti virus protection.
2. All electronic information (text files, data files, executable files, WEB, email, etc.) received, transmitted, and/or stored through Zenergy Connect's communication channels, its network is subject to mandatory anti-virus controls.
3. The use of anti-virus protection tools (checking) must be in continual operation.

4. If a server is to be turned on or off or restarted an anti-virus scan should be carried out manually and the results logged.
5. Use of antivirus protection tools (check) must be performed before installing newly purchased (modified) software, and the results are recorded.
6. Checking information for the presence of viruses is conducted immediately upon its reception or before its transmission.
7. Antivirus protection of hardware is conducted by anti-virus software installed on all network servers and workstations of users.
8. Antivirus definitions are updated automatically.
9. The installation and setup of antivirus software on hardware is done only by authorised officials. The installation, modification (upgrade) of antivirus software on workstations and servers is done by Zenergy Connects's system Administrator.
10. If there is a suspicion of the presence of viruses (for example identifying atypical functioning of software), the official (the user) must conduct an immediate antivirus check of the workstation.
11. In cases of detection of a computer virus (viruses), the user must:
    a. immediately cease work and notify the systems administrator;
    b. disconnect the workstation's network cable and/or disconnect from the office Wi-Fi;
    c. to notify other users who are using the infected software, file(s), database etc.;
    d. if the infected resource is a local file, the systems analyst should then perform an analysis on the device and file;
    e. to take action to remove the computer virus by using antivirus software installed on the workstation;
12. When a computer virus (viruses) is detected, the systems administrator must, with the owner of the infected device, analyse the probable source of the infected file and to take actions for its elimination.
13. In cases where the infection with a computer virus (viruses) is of a mass nature, the administrator, in agreement with the management, may temporarily terminate general access to the infected resources and/or stop the operation of individual subsystems (services). Informs about the actions taken and gives instructions for action to the interested users and officials.
14. In cases of detection of a virus (viruses), the removal of which is not possible with the antivirus software used, the administrator reports and with the assistance of the other administrators (of the network, of the database) takes measures to terminate

access to the workplace or the infected network segment to the general network environment.

11. Operational Control, Event Logging and Monitoring Policy

The operational control tools used in GL Telecom are designed to detect and log all events (user actions, unauthorised access attempts, etc.) that may lead to a violation of the adopted security policies and occur of a crisis situation, and this is carried out operationally by ZC's system administrator.

12. Security policy for identifying incidents

Users must notify the systems administrator immediately of known or anticipated cyber security incidents. The user is prohibited from performing security vulnerability testing without the permission, guidance, and involvement of the organisation's information security personnel. User shall not disclose discovered vulnerabilities or security weaknesses.

13. Security policy for the destruction of information carriers

Once they are no longer needed, media must be destroyed securely and safely using formal procedures.

Formal procedures for secure electronic media destruction should minimise the risk of sensitive information being leaked to unauthorised persons. Procedures for the secure destruction of media containing sensitive information must be commensurate with the sensitivity of the information.

Media containing sensitive information must be stored and destroyed securely and safely, for example by burning or emptied of data for use by other applications within the organisation.

There are procedures in place to determine which items may require secure destruction. It may be easier to arrange for all media items to be collected and securely destroyed rather than attempting to separate the sensitive items.

When collecting media for destruction, consideration must be given to the crowding effect, which can cause a large amount of non-sensitive information to become sensitive.

Care must be taken to ensure that sensitive information is not disclosed through careless destruction of the media.

14. Mobile Assets and Telecommunications Security Policy

Users are responsible for maintaining the security of mobile devices, including but not limited to notebook computers, telephones, PDAs, and others provided to them by the organisation.

In the event that a mobile asset is lost, stolen, or destroyed and it is proven that the person responsible for that asset was negligent in its use, the organisation has the right to seek financial responsibility for the damage caused. Such incidents must be reported to the systems Administrator immediately.

Users are strictly prohibited from storing information that is the property of the organisation on personal devices or any resources that are not approved by the Administrator and configured in a way that ensures the security of the information.

Direct access to the Internet (e.g. cable modem or DSL) through equipment not owned by **Zenergy Connect.** computer equipment owned by the organisation is approved by responsible officials.

15. Remote access policy

Only users who are documented to have a legitimate business or other reason to use remote access should be provided. Users who use remote access should not be provided with the remote access software in an installation form but should be installed on the portable devices by the system administrator.

All remote access points to the organisation's network must be in the approved access zone and approved by the Administrator and only via Zenergy Connect's VPN. The use of modems or remote access solutions, including Wi-Fi Internet for network access via Zenergy Connect's VPN, is permitted when there is a valid business reason.

16. Security policy for equipment outside the office

VPN Policy to be inserted once in place

17. User restrictions

The user must not use any system:

- in a manner that will result in a violation of this and any related procedure, policy, or instruction in the organisation.
- in a manner that will adversely affect the organisation, such as using pirated software or other copyrighted material, stealing passwords, hacking, engaging in

sharing or viewing pornography or other obscene material, or committing other unethical or wrongdoing.

- to load, download or store multimedia and executable files that are not work-related or unauthorised.
- for participation in business activities that are not related to the organisation.
- to participate in gambling.
- for solicitation purposes such as soliciting contributions or soliciting memberships not endorsed by the organisation, charities or soliciting political candidates.
- for attempts to acquire financial benefits using the knowledge of confidential information.
- in a way that would offend, harass or distress a person, for example by uploading, downloading or transmitting sexual comments or images, racial or ethnic jokes or other comments or images that would offend someone on the basis of race, gender, national origin, sexual orientation, religion, political beliefs or disabilities.
- give access to any systems of unauthorised third parties or by any means any way to compromise the security of these systems.
- publicly comment or speculate on the policies, actions, or performance of the organisation.
- publish classified information on the Internet unless it is part of his specific work.
- in a manner that would significantly affect the capacity, integrity, security, or the performance of any system.

User ownership, development, or intentional use of viruses, hacking tools or other harmful software is prohibited.

Only software authorised by the Administrator should be installed on Zenergy Connect's hardware. User may not install software on any Zenergy's hardware.

Users must not attempt to circumvent the security of any of the systems.

18. Organisation rights to monitor systems

Subject to compliance with current legislation, any system and its use by an employee/user can be monitored. Workers not employed under contracts of employment may not be so monitored. Any monitoring such as interception of

communications or monitoring of Internet usage will only be conducted when required for the legitimate interests of Zenergy Connects**.** These interests include:

- ensuring the efficiency and/or security of any system;
- maintaining records of transactions in which our business is involved;
- establishing employee compliance with applicable legal and company policies and procedures or;
- the detection or prevention of crime.

Monitoring will be in accordance with applicable procedures and applicable legal requirements. All data collected as a result of monitoring activities will be processed in accordance with applicable laws and may be disclosed outside of Zenergy Connect in support of or as part of investigations or legal proceedings.

Passwords and usernames are intended to protect Zenergy Connects's business and its information from unauthorised access and not to provide users with personal privacy in their communications.

19. Classification guidelines

Information is classified according to its value, legal requirements, sensitivity, and criticality to the organisation.

Classifications and related information security controls must consider business needs to share or restrict information and the business impacts associated with such needs.

The degree of protection can be assessed by analysing the confidentiality, integrity, and presence of any other requirements for the information in question.

Information often ceases to be sensitive or critical after a period of time, such as when it becomes public. These aspects are to be taken into account.

In general, the classification of information is a shorthand for determining how that information should be treated and protected.

20. Addressing security risks

Before considering risk treatment, Zenergy Connect decides what the criteria will be for determining what risks of disclosure is acceptable. Risks may be taken if, for example, it is judged that the risk of disclosure is low or that the cost of protection is too high for the value of the information to be protected. Such decisions must be recorded.

For each of the identified risks, following the risk assessment, decisions must be made to treat the risk. Possible risk management options include:

- implementing appropriate controls to reduce risk;
- knowingly and purposefully taking risks, provided they are in line with policy of the organisation and risk-taking criteria;
- avoiding risks by not allowing actions that may cause the appearance of risks;
- transferring the associated risks to other parties, for example insurers or providers.
- For those risks where the decision to treat the risk is to implement appropriate controls, those controls must be selected and implemented to meet the requirements identified in the risk assessment. The various types of control must ensure that risks are reduced to an acceptable level, taking into account:
- the requirements and limitations of national legislation and regulations;
- organisational goals;
- work requirements and limitations;
- implementation and enforcement costs related to risk reduction and compliance them with the requirements and limitations of the organisation;
- The need to balance the investment to implement and enforce the types of controls against the potential harm that may result from security breaches.

Control types may be selected from those described in Annex A of the standard, or from other sets of applicable controls. They can be designed as new types to meet the specific needs of the organisation.

An important point for creative work in this direction is to organise the surveillance in such a way that the automated information system can be used to collect evidence.

The types of controls described in this application, such as event logging, may conflict with applicable law, as well as the protection of customer or workplace privacy.

The types of information security controls should be considered according to the specification of the project's system and design requirements. Failure to do so may result

in additional costs and less efficient solutions. In the worst case, adequate security cannot be guaranteed.

It should be recognised that no set of controls can achieve complete security and that additional management actions must be taken to monitor, measure and improve the impact and effectiveness of security controls to support the organisation's objectives.

21. Disciplinary process

There should be a formal disciplinary process for employees who have committed a security breach. The disciplinary process should not be initiated without prior verification that a security breach has occurred.

A formal disciplinary process should ensure that employees who are alleged to have committed a security breach are treated fairly. A formal disciplinary process should provide a graded response that takes into account such factors as the nature and severity of the breach and its impact on the business, whether it is a first or repeat incident, whether the breacher has been properly trained, relevant legislation, business contracts and more factors. In serious cases of misconduct, the process should allow for emergency revocation of duties, access rights and privileges, and immediate off-site escorting if necessary.

The disciplinary process should also be used as a deterrent to prevent violations of the organisation's security policies and procedures and any other security breaches by employees, vendors, and third-party users.

22. Support utilities

Devices must be protected against power failures and other intrusions caused by failures in the supporting utilities.

For IT devices that support critical business operations, an uninterruptible power supply (UPS) is recommended to support system outages or continuous operation.

23. Wiring security

Power and telecommunications cabling carrying data or supporting information services must be protected against interruption or damage.

For the safety of the wiring, the following guidelines must be taken into account:

- network cabling must be protected against unauthorised interruption or damage, for example, by using an underground cable conduit or by avoiding routes through public areas;
- Power cables should wherever possible be separated from communication cables to prevent mutual interference;

Reusing devices

All items of a device containing data/media must be checked to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to destruction.

Devices containing sensitive information must be physically destroyed, or the information must be destroyed, erased, or overwritten using techniques that make the original information irrecoverable, rather than using standard erasure or formatting functions.

Damaged storage devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded.

Information may be at risk if devices are carelessly disposed or reused.

24. Identification of third-party risks

The purpose of the organisation of relations with third parties is to maintain the security of information and information assets that are accessed, processed, communicated with, or managed by third parties.

Before starting business, relationships which involve transfer of sharing of data in whatever form with a third party, an analysis and assessment of the risk associated with them is carried out, after which, based on an informed decision of the management, the relationships in question are initiated. All relationships with third parties are conducted on the basis of concluded contracts, which describe the requirements to each of the parties and the corresponding penalties. Depending on the specific nature of the relationship and certain risks, the contracts with third parties are subject to appropriate formal controls and penalties (as a form of preventive control).

The effectiveness of this process is measured by the number of registered problems in communication with third parties to the total number of contracts with third parties.

24.1. Security when working with customers

GL Telecoms does not provide customer access to its information resources. If such access becomes necessary, all requirements for confidentiality and protection of information are analysed and included in an agreement.

24.2. Security in third-party contracts

In cases where contracts are concluded, part of which is it is necessary to provide access, communication, management, and other activities to third parties, affecting Zenergy Connect's information, the relevant information security requirements are to be included in the contract[s]. All contracts must state that any information that becomes known to the contractor must be kept confidential under normal business confidentiality agreements.

The effectiveness of this process is measured by the ratio of contracts in which information security requirements are included to the total number of contracts in which such requirements should be included.

25. Asset management

The objective is to establish and maintain the necessary level of assurance that Zenergy Connects's assets are properly stored and safeguarded.

25.1. Inventory register of assets

All IT assets related to information security for which Zenergy Connect is responsible are described in the Register (List) of assets. When receiving a new asset that is the property of ZC, it is entered in the register by a person authorised by the manager. When an asset is decommissioned, it is removed from the register. Keeping an asset register does not waive the obligation to comply with all accounting policy inventory and asset management requirements.

The effectiveness of this process is measured by the ratio of the assets entered in the register to the total number of assets under the responsibility of the organisation.

25.2. Liability for assets

Each asset has a personal responsible person who is noted in the asset register.

The effectiveness of this process is measured by the ratio of the total number of assets that have an assigned custodian to the total number of assets.

25.3. Use of assets

All assets must be used for their intended purpose and with the care of a good steward. In case of intentional or negligent destruction or damage to the organisation's assets, appropriate disciplinary penalties are imposed according to the Organisation's Internal Labor Rules. Upon starting work, every employee must familiarise himself with the regulations and internal rules in the organisation and declare in writing that he is familiar with and agrees with them. Current versions of regulations and internal rules are available in the organisation.

The effectiveness of this process is measured by the total number of damaged assets due to the fault of employees of the organisation to the number of employees disciplined for these offenses.

26. Equipment security

The purpose is to prevent loss, damage and exposure to risk or disruption of Zenergy Connect's activities.

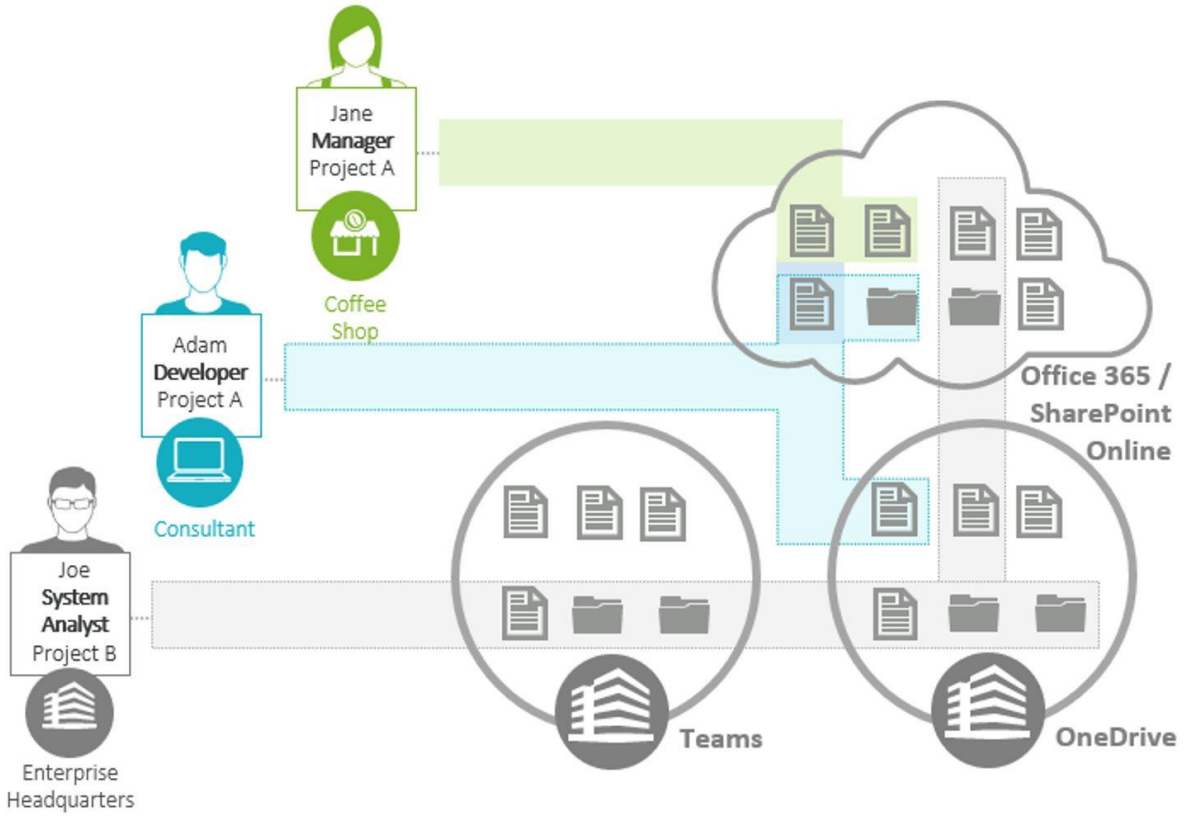
26.1. Equipment maintenance

All IT equipment is maintained by qualified in-house personnel and/or qualified external consultancies according to standard practices.

The effectiveness of this process is measured by the response time when maintenance is needed. The second a measure of the effectiveness of the process is the number of regular preventive maintenance of the equipment.

27. Network security management

The goal is to ensure the protection of information in networks, as well as the protection of structural equipment.



27.1. Network controls

All Zenergy Connects workstations network through, run on and are connected to Window's business 365 and all data is held remotely using Microsoft share point that is protected from unregulated access via dedicated security protocols. These systems have anti-virus and malware checking systems integrated into the systems.

27.2. Security of network services

GL Telecoms uses only the standard network to connect to the systems listed in 27.1 above. The connection within the offices is via a dedicated firewall. The firewall of the router and the controls are built into the operating systems. Throughout devices have anti-virus software.

28. Access control to operating systems

The goal is to prevent unauthorised access to operating systems.

28.1. Initial authentication security procedures

Access to the operating system at boot-time is accomplished by authenticating with the username and password with which the user is registered in the system user access list. When entering the password, the authorised users should not allow it to become known to third parties. Anonymous log-on and guest account

authentication, as well as password-less user accounts, are not allowed and are not configured on operating systems. The effectiveness of this control is measured by the available gaps (anonymous log-on, active guest account, user accounts without a password, etc.) discovered during regular audits.

28.2. User identification and authentication

Each user has his own unique username and password (see password protocols above), with which the user gets access to the information resources of Zenergy Connect and, in particular, to the operating systems. An up-to-date list of users and their usernames is available from the responsible administrator.

28.3. Abort inactive sessions

For each system used, the time to cut off inactive sessions is determined by ZC and is within 30 minutes. In the absence of such a configuration by the provider, the session is automatically terminated when the session key expires (e.g. with SSL).

29. Control access to information and applications

The aim is to prevent unauthorised access to the information stored in the applications used.

29.1. Limiting access to information

Information stored within the organisation's SharePoint information structure is accessible only to those expressly authorised. Information can only be accessed through the SharePoint channels defined and physical access from offices.

30. Security in the development and maintenance process

The purpose is to maintain the security of software and information.

30.1. Change process control

If there is a need to change software resources used by ZC, this change is made by the responsible internal support staff.

The change is accepted by the security officer or responsible system administrator/user after it has been demonstrated by the external contractor that the change is successful and the relevant software package is working.

30.2. Technical review of applications after changes in operating systems

If there is a need to change the operating systems used by the organisation, this change is made by the administrator.

The change is accepted after a functionality test is performed by an admin team and it is ensured that the change is successful, and the relevant software package is working.

30.3. Limitation on changes to software packages

System changes are usually made during automatic updates of operating systems and anti-virus software.

30.4. Information leak

Given the environment in which ZC's data is stored, as well as the number of people having access to it, as well as the fact that everyone working at ZC has agreed in writing to comply with the requirements for confidentiality of information and is familiar with corresponding sanctions, if these requirements are not met, management believes that it is not necessary to introduce additional controls to prevent information leakage.

The risk of information leakage very low and therefore is considered acceptable depending on the risk assessment made, as well as the fact that Zenergy Connect does not work on networks with highly classified information.

30.5. Software development outsourcing

If software development is necessary, an analysis and risk assessment is prepared, based on which a decision is made whether to outsource development and what clauses to include in the development contract.

31. Management of technical weaknesses

The goal is to reduce the risk of someone taking advantage of published information about technical weaknesses and gaps. Technical weaknesses are to be identified during risk analysis and assessment, during regular preventive maintenance and checks by the administrator, or if a security incident occurs. When weaknesses are identified, they are reported to the security officer, who includes them in the risk analysis and assessment, and based on the result, a management decision is made to address the respective weakness.

32. Compliance with legal requirements

The requirement is to avoid inconsistencies with legal and normal business requirements, as well as with regulatory or contractual ones.

32.1. Intellectual property rights

All users are prohibited from installing unlicensed software and using other products, which use constitutes an infringement of intellectual property rights.

Violation of this requirement shall be treated as a disciplinary offense and shall be punished as such.

The effectiveness of this control is measured by the ratio of the number of detected products infringing intellectual property rights and/or the number of imposed disciplinary punishments to the number of users.

33. Record protection

All records of ZC's activities are stored in the SharePoint information systems that are administered by the company.

34. Protection of personal data and other personal information

Zenergy Connect collects personal data and creates files of its employees and workers which are stored at ZC's premises with limited access in a locked cabinet and for some data on ZC's SharePoint data storage system. GL Telecoms is a registered with the Data Protection Office for the use of personal data in England.

35. Compliance with the requirements of security standards and policies and technical compliance

The requirement is to ensure all systems and devices comply with ZC's security policies and standards.

35.1. Compliance with the requirements of security standards and policies

It is the management's responsibility to ensure that all employees work in accordance with the requirements of the ISO 27001 and Cyber Essential's Plus information security standards.

Technical compliance check

Once a year, ZC shall be audited for technical compliance with the information security requirements set out herein. The inspection takes place under the control of the head of the organisation, and its result is documented in writing.

36. Information systems audit considerations and controls

The goal is to achieve maximum efficiency and minimal disruption to the normal work process during an information systems audit.

Before conducting a security audit, the auditor should prepare an audit plan and a detailed description of the audit process, as well as prepare a work program (checklists) for conducting the audit and a complete list of required documents and references. These documents are provided to the head of the organisation, who performs an analysis of how the audit process will affect the work of the organisation. Based on this analysis, a report is prepared.

37. Supplier relationship policy

The responsibilities of the selected suppliers are defined in the agreed contractual agreements.

As may be required by management, designated suppliers shall implement security measures in accordance with established policies and procedures of the procuring organisation.

37.1. Information security in relationships with suppliers, ensuring protection for organisational assets

Information security requirements that mitigate the risks associated with supplier access to ZC's assets are agreed and documented with the supplier. These actions are coordinated with suppliers and documented.

Applicable information security requirements are to be introduced and agreed upon with each supplier who may have access to Zenergy Connect processed, stored, and distributed information. Agreements with suppliers include requirements addressing information security risks associated with the supply chain of information and communication technology products and services and the product supply chain.

37.2. Management of the provision of services by suppliers. Maintaining a high level of information security when delivering services through supply contracts

Service providers are regularly monitored, reviewed, and audited at Zenergy Connect - no less than once a year. Changes to the provision of services by suppliers, containing the maintenance and improvement of existing information security policies, procedures and control mechanisms, are managed considering the critical nature of the information, systems and processes related to the activity and the reassessment of risks.

38. Backup policy

Backups of ZC's data including emails are managed and administered by the administrator. The organisation is guided in this process by the detailed Backup Procedure.

39. Policy for secure systems

The purpose of this policy is to define the application of Secure Systems Principles and ways to prevent creating conditions for potential inconsistencies in ZC's operations. The goal is also aimed at determining the main mandatory principles of system engineering at all stages of our information system.

Zenergy Connect defines our engineering principles for secure systems, documented, maintained and applied to all information system development efforts. Basic guidelines for implementation when building secure systems, the engineering principles approved in ZC must be followed.

The architectural solution is built in a way that allows:

- Separation of usernames and passwords from application code and their ability to encryption on demand;
- Separation of the database from the application server in order to prevent direct access to it if the latter is compromised;
- Separation of the WEB server from the application server (if the security level requires it) in order to prevent direct access to the system should the WEB server/data storage be compromised;
- Wherever personal or sensitive data is entered, the connection is protected with SSL encryption with a respected SSL certificate;
- Wherever there is a connection with external systems, it is done with SSL encryption with a certificate and the latest trends for building WEB Service interfaces are used;
- If it is necessary to connect different applications, the current industry acceptable mechanisms are used to ensure access and secure transmission of the various attributes;
- When the system requires external access, it is limited only to the necessary ports and protocols, as well as IP addresses;
- All systems providing public services are located in the access area of outsiders;

- Every action in the IT system[s] are recorded in an action log for subsequent verification in need.
- Security must be designed into all architectural layers (business, data, applications, and technology) to balance the need for information security with the need for **availability.** Periodic (according to the intensity of the project) reviews of the system[s] are made in order to ensure its necessary quality.
- The implementation of new technologies requires security and design risks to be analysed and should be reviewed as familiar usage patterns.

These principles and established development procedures shall be reviewed as necessary to ensure that they will effectively contribute to increasing the effectiveness of security standards within the development process. They are regularly reviewed to ensure that they remain up-to-date in terms of combating any new potential threats and in the other applicable development technologies and solutions that will be implemented.

Defined security engineering principles are implemented wherever possible through outsourcing of the information storage and retrieval, the development of the systems or through the contracts and other binding agreements between Zenergy Connect and any external developer and/or subcontractor to whom it is assigned.