ADASTRA

Information Security Policy Adastra Group

1. Introduction

Adastra Group has began the task of creating, implementing, operating, monitoring, maintaining and improving on an information security management system.

Adastra's current vision considers information security (IS) as one of the company's top priorities. In this way, the company maintains client confidence in our ability to not only provide quality services, but also to protect their information by implementing appropriate security measures such as processes, tools and a reliable infrastructure. Adastra Group strives to be not only a supplier but also a first-class partner for its customers. Adastra wants to be in a position and have a reputation where they are a partner that is sought after and in demand for their services. Therefore, Adastra maintains and regularly certifies an ISMS system to enhance information security and manage the overall risks of the company's operations.

The Information Security Policy defines the basic strategy, objectives and principles relating to the company's information security, and defines the basic security rules for the operation, use and maintenance of information and communication technologies. The Policy ensures the required level of information protection and to minimize the damage resulting from potential security incidents.

Most of the security measures implemented by Adastra Group to protect sensitive client information are based on contact agreements with clients and are governed by the requirements set by the clients themselves. For clients who do not set clear information security requirements or whose requirements have gaps, Adastra Group applies the security standard described in Adastra's information security policies and procedures, including this ISMS policy.

The Information Security Policy is a binding document with which all employees, subcontractors and, to the extent necessary, third parties who have agreements involving the access, processing, disclosure or management of the company's information, or the supply of products or services to information processing equipment, must be familiar.

1.1 Purpose and Scope

The Information Security Policy document is the basic basis for establishing, implementing, operating, maintaining and improving the Information Security Management System (ISMS). This document is intended for use by Adastra Group SE and business entities under its control ("Adastra").

2. ISMS Goals and Objectives

There are several goals for the ISMS in Adastra:

Support the business development process (both local and international) in maintaining a protected project environment and complying with all client contract agreements.

The objectives to measure this goal are:

- Support sales activities and provide full and on-time information to present the capabilities of the Adastra information security framework. Agree on the appropriate IS controls to be implemented for each client from Adastra Group as part of the service delivery process.
- Ensure the needed infrastructure changes occur and minimize delays in project ramp up processes due to unsecure infrastructure.
- Ensure that all consultants who are members of the involved project teams are aware of the project IS requirements and restrictions. Make sure that all consultants pass proper security awareness training no later than a week after their start date.

Support the service delivery process and minimize the number of security incidents.

The objectives here are:

Identify and assess IS risks associated with each project and treat those risks so that they are acceptable. Keep a risk log for all projects in the company.

Handle all security incidents according to the Security Incident Response Plan. Keep the security incidents resolution on the agreed SLAs depending on the incident priority and severity.

Maintain a fully functional internal audit to check regularly for potential issues in the service delivery process.

2.1 Evaluation of the Effectiveness of the ISMS

Adastra has created a system of controls to monitor each of the goals and objectives set in section 2.1, *ISMS Goals and Objectives*. The controls include, but are not limited to:

- Regular review of the ISMS operation at the executive management level

- A regular internal audit of the company ISMS identifying potential non-conformities with the different IS policies or with the ISO 27001, TISAX or SOC2 requirements

2.2 Review of the Adastra ISMS Policy and Continuous Improvement

Adastra's ISMS policy should be reviewed on an annual basis following its implementation. Main objectives for the review process are:

- involvement of all members of the Adastra executive management team;
- discussion of the available information about issues or areas for improvement of the ISMS policy;
- analysis of cases where non-conformity with the established IS requirements is identified;
- following up on activities to close the identified issues/gaps.

2.3 Responsibilities

2.3.1 Management Responsibility

The management of each Adastra Group company makes the following commitments under the information security policy in accordance with the company's requirements:

- To manage and continuously improve the information security management system throughout the company.
- To apply a policy based on the principles of confidentiality, availability and completeness of information, including compliance with standards, legislation and moral principles.
- Regularly assess the achievement of objectives and targets based on risk analysis and ensure an appropriate and effective approach to the management of security incidents.
- To continuously raise the awareness of employees and thereby maintain a high level of information and overall company security.
- To apply the information security principles convincingly and firmly to contractors and third parties, thereby demonstrating the company's professional approach and market position.

- To provide customers and contractual partners with the necessary level of assurance in the handling of their information assets by implementing an information security management system.

2.3.2 Employee Responsibility

Any employee who has been granted access to information resources for the purpose of carrying out his/her/their work activity assumes responsibility for the safe handling of these resources and for the protection of information within his/her/their area of responsibility. The established, adopted and approved Information Security Policy and related security documentation is binding for all users with access to information, regardless of their positionor role in the company. In accordance with the applicable legislation and regulations, all users bear their share of responsibility for compliance with or violation of the rules with which they have been acquainted.

All employees are obliged to respond in the prescribed manner to faults, malfunctions and safety incidents that occur and to report them in accordance with the relevant policies and guidelines. This means reporting security incidents and informing those responsible of any weaknesses in the ISMS immediately.

2.4 Main Principles for Information Handling and Security

- Maintain the security of the organization's information that is accessed, processed, or shared by external entities
- Ensure that information receives an appropriate level of protection
- Ensure that employees, contractors, and third parties are aware of their responsibilities so that appropriate candidates are selected to reduce the risk of human error, theft, misuse, fraud
- Prevent unauthorized physical access to designated areas of the organization
- Prevent loss, damage, theft of information or disruption to the organization
- Protect the integrity of software data
- Ensure controlled access to information
- Maintain the security of software and application system information
- Ensure secure data backup

2.5 Consequences of a Breach of the Information Policy

- Violations of this Information Security Policy by company employees are considered a security incident that affects information security and must be addressed accordingly.
- The causes of breaches of the information policy must be analyzed and effective action taken to learn from these incidents.
- All such breaches are recorded and subsequently managed.

2.6 Risk Management

The purpose of information security risk management is to establish a process for improving the effectiveness of measures to eliminate identified unacceptable information security risks.

The security director must ensure that Adastra conducts a risk assessment review once a year or in the event of significant organizational and technical changes.

The security director must ensure that the residual risk and the level of acceptable risk are reviewed in light of changes in the organization, technology, the organization's business objectives and processes, identified threats, the effectiveness of the measures in place, the regulatory and legal environment, changes resulting from contractual obligations and changes in the social climate.

The risk analysis is performed according to a methodology approved by the company's senior management.

Changes in the provision of services by external entities shall be managed with regard to the criticality of the organization's systems and processes and shall be part of a recurring risk assessment.

2.7 Human Resource Security

2.7.1 Prior to Employment

2.7.1.1 Hiring Procedure

The primary objectives for the hiring procedure are to ensure that employees, interns, contractors, and third-party users:

- Understand their responsibilities
- Are suitable for the roles they are considered for
- The following goals must be achieved during the hiring process:
- Check for availability of satisfactory references
- Check for completeness and accuracy of the applicant's curriculum vitae
- Confirmation of claimed academic and professional qualifications
- Independent identity checks (passport or similar document)

2.7.1.2 Screening

All candidates for employment, interns, contractors, and third-party users should be adequately screened according to the national legislation, including:

- Criminal background checks
- Review of employment history
- Gap analysis for any periods between employment

Additional screening (like an international background check) can be requested when clients have special requirements for people working on their projects.

2.7.1.3 Terms and Conditions of Employment

Security responsibilities must be addressed prior to employment in adequate job descriptions and interims and conditions of employment.

2.7.2 During Employment

2.7.2.1 IS Awareness Training

Adastra has set up a special IS awareness training program. The main goal of this training program is to ensure that employees of Adastra understand the sensitivity of our's and our customers' information resources and their responsibilities to protect those resources, applying information security policy and procedures as per policy.

Specific objectives of this program are:

- to define the organization strategy and implementation plan for establishing a reasonable level of staff security awareness;
- to define the scope of the training and introduce an effective testing mechanism;
- to assist employees in using safe and secure practices according to company policies and applicable legislation;
- to answer any questions about information security requirements, policies, and procedures; and
- to promote security awareness at all levels in the organization.
- The IS awareness training is mandatory for all employees in the company and must be passed as follows:
- In the first week after hiring
- On an annual basis
- In cases when there are important changes in the training materials

2.7.2.2 Disciplinary Process

The disciplinary process in Adastra is compliant with the national law. In addition, the disciplinary process should also be used as a deterrent to prevent employees, interns, contractors, and third-party users in violating company security policies and procedures, and any other security breaches.

2.7.3 Termination or Change of Employment

2.7.3.1 Termination Procedure

The procedure for terminating an employee's contract is to strictly follow the articles for contract termination in the national law. In these cases, it is in particular necessary to ensure terminated employees:

- Return all company information assets and used equipment
- Remove all access rights that have been granted
- Inform clients if the employee was involved in projects with them, ensuring that all access to the client's systems have also been removed

Ensure the reassignment of the departing employee's responsibilities.

2.7.3.2 Return of Assets

The termination process must include the return of all previously issued software, company documents, and equipment. Other organizational assets such as mobile computing devices, credit cards, access cards, software, manuals, and information stored on electronic media also need to be returned.

In cases where an employee, intern, contractor, or third-party user has knowledge that is important to ongoing operations, that information should be documented and transferred to Adastra representative(s).

2.7.3.3 Removal of Access Rights

Upon termination, any access rights granted to the departing employee must be properly listed and analyzed to determine:

- Whether it is necessary to remove access rights. Changes in employment should be reflected in removal of all access rights that were not approved for the new employment.

- Whether there are accounts accessed by the departing employee that should remain active. In these cases, the passwords for accessing those accounts must be changed upon termination of the previous contract.

The access rights that should be removed or modified include physical and logical access, keys, identification cards or any other information assets.

2.8 Personal Safety

The purpose of personnel security is to reduce the risk of human error or intent to misuse information assets.

- Employees are obliged to maintain the confidentiality of the facts they have become aware of in the performance of their work tasks or in direct connection with them, and this obligation continues even after the employment relationship has ended.

Staff are required to be familiarized with the Information Security Policy as part of their initial training and periodic training (more in point 2.6. above).

- Adastra employees who work at customers' sites and whose computing devices are connected to customers' computer networks must primarily comply with the regulations established for operation on the customer's computer network but must not violate applicable Adastra regulations.

- Employees must be familiar with security incident reporting procedures.

2.9 Physical Security

The purpose of physical and environmental security is to prevent unauthorized physical access to ICT equipment, information and data.

Access from publicly accessible areas to Adastra Group companies' premises containing information or information processing facilities must only be possible via security perimeters (such as electronic access control or reception).

Access to secure areas (e.g., server rooms) must only be granted to authorized persons using an appropriate access control system.

The provision of fire safety according to the laws and regulations of the country concerned must be regulated by a specific internal organizational directive within the Adastra Group.

IT staff must ensure that all devices containing storage media, sensitive data and licensed software are removed or securely overwritten before disposal or reuse.

Critical data transmission and processing equipment (e.g. servers and active network elements) must be located in secure areas and protected from power failures and other disruptions caused by the failure of support services (e.g. data leases or Internet connections).

Each employee is required to follow the "Clean Desk Policy“

2.10 Communication Safety Management

The purpose is to ensure the correct and secure operation of information processing facilities.

- Operating procedures for both users and IS administrators (local key users) shall be documented and maintained and shall be available to them as required.
- Protection against malicious code (computer viruses, etc.) must be used on all devices and servers connected to the company's network;
- Data in the IS must be backed up regularly to ensure data and system recovery in relation to maintaining Adastra's core functions;
- Recovery procedures must be developed following failure or failure of the information processing and storage system;
- System capacity (disks, network, memory, processor load) must be monitored regularly by IT staff and expansion planned and implemented in a timely manner based on their suggestions;
- Computer networks must be appropriately managed and controlled for security;

The data distribution switchboard must be inaccessible to unauthorized persons and all data sockets must be located in Adastra's internal premises;

- Security features, service levels and management requirements for all network services must be identified and included in network service agreements;

IS operations must be monitored, and audit trails containing error messages and other security significant events must be captured, retained and protected for a specified period of time so that they can be used for future investigations and for access control monitoring and event logging purposes;

Defined rules and procedures must be developed and put into practice to protect information in the interconnected information systems between Adastra Group companies.

- Hard drives and removable media must be removed or information must be securely removed from them before the equipment is taken out of service or sent for servicing.

Unauthorized eavesdropping on traffic or intrusion into Adastra computer networks is prohibited.

IT must establish formal policies or procedures if necessary, to protect against the risks of using mobile computing and communications devices.

- IT must establish formal policies, procedures where necessary, for working remotely with information systems.

The clocks of all Adastra domain information processing systems must be synchronized with an approved source of accurate time.

2.11 Access Control

The purpose of access control to Adastra information systems and resources is to ensure that only authorized users have access to them. Access to these resources is governed by rules that specify procedures for authorizing, establishing, modifying and revoking access rights.

- All users must be assigned a unique identifier (user ID) and the password management system must ensure the use of quality passwords.

Users shall only have access to those network and application services for which they have been specifically authorized to use.

- Access permissions shall be used by users only for the purpose for which they were created.
- A user shall not provide the assigned access permissions to another person.
- A user shall not attempt to obtain access rights that have not been granted to him/her by any means.
- In the event of termination of employment, all access privileges must be revoked.

- In the event of a change of position within the company, IT must, at the direction of HR, reduce access rights to a minimum level and then set up new access rights using the procedure for establishing access rights for a new employee.
- The granting and use of privileges must be restricted, controlled and recorded.

Access by remote users to Adastra network or application services shall be authenticated appropriately.

- Inactive sessions shall be terminated after a specified period of inactivity.
- For high-risk applications, a connection time limit must be used to provide additional security.
- Access to tools designed for auditing information systems (vulnerability scanning tools) must be protected to prevent their possible misuse or compromise.

Before external parties are allowed and granted access to Adastra information and processing facilities, risks must be identified and appropriate measures implemented to cover them.

- Information owners must review user access rights to information at least once a year.

Logged-in personal computers, servers or other devices connected to Adastra's network must not be left unattended and must be protected by key, password or other measures when not in use.

2.12 Managing Change in Society from an Infrastructure Security Perspective

Any changes in Adastra, its processes and any other changes that may have an impact on information security must be assessed from an information security perspective and linked to the establishment of appropriate security requirements.

2.13 System Development and Maintenance

The purpose is to enforce information security in the entire life cycle of operating information systems, from the design, development, testing to the actual operation and maintenance.

The implementation and modification of Adastra information systems must be linked to the establishment of appropriate security requirements.

Separation of development and testing resources from operations must be ensured.

In Adastra information systems applications, the input and output data of the applications shall be checked for correctness, including the integration of data validation checks into the applications.

- Requirements for ensuring authentication and message integrity shall be established for each application and appropriate measures identified and implemented as necessary.
- IT shall have procedures in place to control the installation of software on operational (production) systems.
- Test data must be carefully selected, protected and controlled.
- Access to source code must be restricted.

In the event of changes to operating systems (versions, configurations), critical applications must be reviewed and tested to ensure that the changes do not adversely affect the operation or security of the organization.

- A policy for the use of cryptographic measures to protect information must be developed and implemented.
- A key management system shall be in place to support the use of cryptographic techniques.

2.14 Cyber Security Incidents

The purpose is to create such technical and organizational mechanisms in the organization that would reduce the probability of security incidents and minimize their consequences in case of their occurrence.

The following situations are considered to be a security incident:

- Disruption of the functionality of the IT infrastructure by natural disaster, malfunction, negligence or deliberate action
- Deliberate collusion (espionage, sabotage or embezzlement) or suspected collusion
- Unauthorised use of the system or unauthorized access to data
- On the discovery of system vulnerabilities
- To detect the presence of a malicious program
- Misuse of the infrastructure of companies belonging to the Adastra Group (active network elements, PCs, laptops, servers) for attacks against other entities
- Loss of a laptop or other mobile device on which non-public information is stored by Adastra Group
- Disclosure of the access password or private key of the certificate to another person or suspected compromise of such access data
- Any other failure to comply with the requirements of the information protection directives

All persons working with Adastra Group's information systems must be instructed on the actions to be taken in the event of a suspected security incident, in the event of a malfunction or limited or altered functionality of Adastra Group's information system services.

All suggestions from employees must be received, evaluated and archived. Depending on the severity of the complaint, processes leading to remediation are initiated.

The classification of security incidents, rules, procedures and responsibilities are defined by Adastra Group companies in their internal regulations.

2.15 Business Continuity Management

The intention of Adastra's Senior Management is to ensure readiness to deal with crisis situations and to maintain core functions to the extent necessary for Adastra to function.

Responsibilities for business continuity management must be clearly defined.

Business continuity management must cover all areas relevant to the functioning of the company, in particular those mentioned below:

- Internal systems, activities and processes
- Customer service delivery (project management)
- Services provided by the supplier

The security objective is to ensure that designated personnel are prepared, trained and ready to perform activities related to crisis management.

The transition to crisis management is the responsibility of the company's senior management.

The adoption of preventive measures to maintain essential functions is the responsibility of the company's senior management.

2.16 Compliance with Legal and Contractual Requirements

To secure information in Adastra, all relevant legal and contractual requirements in each country must be clearly defined and documented. An inventory of applicable national laws and regulations relating to information security issues must be maintained within Adastra.

Cryptographic measures must be used in accordance with relevant conventions, laws and regulations.

Adastra Group shall comply with copyright provisions and the terms of software vendors' licensing arrangements.

Adastra Group must take and implement measures to ensure the protection of personal data in accordance with laws and regulations.

2.17 Responsibility, Change Management

Every employee and subcontractor shall be familiar with this document and shall be made aware of the need to comply with it.

History of the document:

Version:	Date:	Author:	Changes:	Authorization: