DoControl.

One SaaS to secure all other SaaS

Procedure 02 - Information Security Policy
V 1.0 September 2020

Information Security Policy

Document Revision History

Author	Edition	Comments	Date
Ron Peled	1.0	First draft	Sep 13, 2020
Ron Peled	1.1	Operational adjustments	Sep 13, 2020
Omri Weinberg	1.1	Reviewed and approved	Sep 13, 2020

Approvals

Name	Title	Comments	Date
Omri Weinberg	CRO	Reviewed and approved	

DoControl.

One SaaS to secure all other SaaS

1. General, Company Profile and Core Processes

Company Profile: DoControl is an innovative cloud-based software company that develops an advanced, agentless solution for protecting Cloud and SaaS applications.

Core Processes:

A. Research & Data Science – continuously investigate and study the industry leading SaaS and Cloud platforms as well as user and data protection capabilities.
B. Product and Software Development – translating market research and customers' needs into a best of breed working product.
C. Sales – activities related to selling the Product to customers.
D. Solution Delivery – maintaining the infrastructure and SaaS environment that facilitates customer operations and integrations.
E. Security - constantly keep track of data protection trends, risk and solutions to help protect the company, products and customers.
F. Customer Support – track and resolve potential product / service issues for customers.

2. Purpose, Overview and Applicability

1. This policy was designed to help DoControl and its employees reduce security risks.
2. All DoControl employees are expected to adhere to the Information Security policies and protect DoControl's data assets as part of their day to day activities.
3. The primary objectives of this policy are outlined below:
    a. Help ensure that the company's information assets are properly protected from unauthorized access, alteration and/or destruction.

b. Help ensure that such protection is balanced and consistent with the company's business requirements.

c. Help ensure that industry best practices are implemented in order to provide risk guidance and reduce the overall risk of security vulnerabilities.

d. Provide a concise set of standards in order to attain consistency across the information infrastructure in regard to securing systems and networks.

e. Providing a security management system that supports compliance with the Israeli law and the General Data Protection Regulation and future applicable laws and regulations.

f. Provide a security code of conduct for employees and managers alike.

4. **Overview and applicability**

a. This policy covers the security best practices applicable for protecting the company’s systems, infrastructure and information.

b. This policy applies to all company’s personnel including, but not limited to, employees, contractors, consultants, and temporary staff.

c. All the company's personnel are expected to become familiar and comply with this policy.

d. Failure to comply with this policy may result in disciplinary actions, including termination.

5. **Scope**

a. The implementation of the information security system in the Company applies to all the facilities, operations, projects and work procedures within the company. It will be implemented in each and every location where employees operate.

b. The information security system is externally audited in the company primary location in Israel, but shall apply to all employees regardless of location as applicable.

c. This information security policy and the standards derived by it, apply to all the information systems and business procedures supporting and processing it, as they were identified and mapped during the risk evaluation review held by the Company.

3. Board and Management Commitment

1. DoControl's management and board of directors are committed to maintain a high standard of information security by their responsibility for proper management of the company.
2. The management is obligated to provide adequate resources to maintain an appropriate level of information security in the company and to budget the annual work-plan.

4. Policy Goals

1. Protect company and customer data from unauthorized and/or malicious activity by effectively and efficiently enforcing an information security policy.
2. Enable the business strategy through security guidance, privacy guidance and risk management.
3. Help the company maintain the confidentiality, integrity, and availability of information.
4. Serve as the basis for information security procedures and controls.
5. Provide guidance on identification and management of information security risks.

6. Define the methods for enhancing security awareness across the company.
7. Define the required baseline for an annual work-plan that includes the following:
    a. Scoping, purchasing, installing, and integrating security controls.
    b. Maintaining information security controls.
    c. Maintaining a risk assessment program.
    d. Performing special projects.

5. Information Security Business Principles

1. Create a security culture through information security governance.
2. Assess risks through understanding, evaluating, and testing.
3. Ensure effective implementation of the critical information security basics by following policies, procedures, and guidelines.
4. Enforce the information security policy through technological processes where applicable, education, monitoring, and metrics.
5. Adhere to applicable regulatory requirements including international & local laws.

6. High Level Primary Risks

The company processes information of business, financial, and personal nature. Vulnerabilities (technical, logical or procedural) may affect the confidentiality, integrity, and availability of that information. The company's primary information security risks are listed below:

Technological risks:

1. Impacting customer data and/or privacy due to unauthorized access or leak.
2. Misconfiguration or lack of ability to detect malicious activity.

3. Decrease or interruption in system or asset availability/credibility.
4. Data corruption in production environment information systems, which could lead to invalid actions or faulty decision taking
5. Impacting the survivability of the company's systems due to technical failure.

Human factor and organizational risks:

1. A security breach pertaining to the following: Employees, customers, internal R&D documentation and specifications, financial data, intellectual property.
2. Errors leading to information security breach.
3. Malicious behavior by authorized personnel or third parties.
4. Transferring certain types of Information in an insecure manner.
5. Loss or theft of IT equipment and/or confidential Information.
6. Failing to comply with applicable legal or regulatory requirements
7. Unauthorized access to company's facilities or restricted areas.

7. Key elements of the ISMS

1. Information security measures and methods are implemented to minimize risks and shall be adapted based on the risk and sensitivity level over time.

2. In order to achieve an effective information security program, the following elements are implemented:

    a. Prevention – controls designed to prevent malicious or accidental damage to company's infrastructure and data.

    b. Detection – detecting issues that were not blocked by the prevention layer.

    c. Response – a reaction or corrective action in response to detection.

        - Real time – by changing the prevention capabilities of the system.
        - Post event – shall be based on information logged during the event, analyzing it, and drawing conclusions.

d. Documentation – allow analyzing the events (prevention, detection, or reaction events) to allow a broad perspective of the event.

e. Effectiveness confirmation - if corrective actions were implemented, their effectiveness should be measured and tested.

8. Organizing Information Security

In order to perform the requirements of the policy, the company shall define a suitable framework, based on the following:

1. Information security steering committee:

    a. The information security steering committee is the highest body authorized to approve changes to the policy and to decide how to implement it as a representative of the management and technological factors, while assisting in external consultants and specialists.
    b. Members of the committee include the CEO, CTO, and CISO.

    c. Committee roles:
        - Approving the information security policies and tracking its adoption.
        - Approving and monitoring the security work-plan
        - Approving information & system classification levels
        - A deciding authority in cases of dispute on information security topics.
        - Lead the company response and actions in case of a breach.
        - Convene at least twice a year for status review.

2. Information Security appointee / CISO:

    A management member responsible for information security in the Company. Within DoControl, the CTO is also the CISO with the following roles:

    - Providing the board of directors an annual information security review.
    - Presenting information security topics to the management.
    - Leading the information security Steering Committee.

- Implementing the information security policy
- Initiate and implement an annual work plan.
- Responding to Information security incidents.
- Conducting information security awareness training.
- Establishment of security processes for information systems.
- Involvement in technological changes in computer systems.

9. Data classification

The company maintains two classes of data **Confidential** and **Public**.

1. All documents created within the company are considered confidential, unless specifically designated otherwise. Document owners should label it accordingly.
2. There are two types of confidential information that require extra care: Customer Confidential and Personally Identifiable Information (PII). Such Information shall be registered and protected as required by applicable law and contracts.
3. The company's **confidential Information**:
    a. Internal Confidential - Information that should stay within the company, protected from external access. If such information were to be accessed by unauthorized persons, it could influence the company’s operational effectiveness, cause a financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence and reputation.
    b. Customer Confidential Information - information that was provided to the company by its customers under non-disclosure agreements or information pertaining to the customers' employees, generated within the process of providing customer service. All such customer confidential information should be protected from external access. Unauthorized access could influence the company's operational effectiveness, financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence and reputation of the company.

c. Personally Identifiable Information (PII) relates to any type of information that may be used to identify specific people and their personal traits as defined by applicable laws and regulations. Such data will be considered as sensitive data and will be limited in usage within the company, accessible on a need to know basis only.

4. **Public Information** (non confidential): Marketing, social media or customer facing material that were pre-approved by management to be publicly disclosed. This does not include any information that could be used for competitive purposes against the company.

10. Risk Assessment Approach

1. A periodic risk assessment is the basis for an ongoing information security.
2. The assessment is applied to both technological and non-technological aspects.
3. Risk assessment shall include internal and external reviews, penetration tests as well as system configuration reviews and reference to security incidents if any.
4. The Risk Assessment will strive to represent risks based on the potential risk and occurrence likelihood.
5. The assessment shall aid with workplan establishment aimed to minimize the risks.

11. Human Resources Security

Aspects of information security are implemented by the company across the employment lifecycle as outlined below:

1. Prior to the Employment:

    a. The company is responsible to assure that its employees (and contractors) are competent for their intended position and understand the responsibilities imposed on them in order to prevent events of failure, fraud or abuse.

b. The management shall define with respect to each of its office holders:

- The necessary qualifications
- Responsibility and authority
- Requirements of reliability
- Access rights to information systems

c. Employee / contractor reliability will be determined through a process of interviews and reference checks.

d. Each employee / contractor shall sign a confidentiality agreement that outlines the information security and privacy expectations as a condition for employment.

2. Within the Process of Employment:

a. Employees and contractors will be made aware of the common information security threats as well as the policies and practices expected of employees to reduce and help prevent such risks.

b. All employees will undergo periodic training or will be notified to help increase their awareness of the following topics at least once a year: Information security policy highlights, common threats, acceptable use of assets, data and privacy protection practices and incident reporting.

c. New employees will obtain an information security awareness summary or debrief as part of their on-boarding process to become familiarized with the company's policies.

3. Termination of Employment or change of roles:

a. Employees or contractors leaving the company or changing roles will do so in an orderly and secure manner.

b. Upon transition between positions access permissions that were granted in the previous role will be examined and adjusted for the new role, or revoked.

c. Upon termination of employment the following actions will be performed:

   i. Revoke access permissions to all systems and data assets.

   ii. Confirm the return of company assets, data and equipment.

   iii. Remind the employee on their confidentiality obligations.

12 Workstation and Server Security

A. The following controls will be effectively and actively implemented on all **workstations**:

1. Full disk encryption and time based password protected screen savers.
2. Automatic installation of Security updates and OS patches.
3. Software based Firewall, Intrusion Detection and Anti-Malware active at all times.
4. Software installation is subject to the CTO / CSO approval.
5. Where applicable – employees will run with non-elevated permissions.
6. Workstation configuration will be performed by authorized personnel only. Disabling security controls may result in disciplinary action.

B. The following controls will be effectively and actively implemented on all **Servers**:

1. Access to servers is restricted to the minimal number of authorized personnel.

2. Incoming traffic will be filtered by a Firewall and/or Access List with strict policy of minimal ports enabled.
3. Servers should be hardened (no default passwords, installed with the minimal packages and services required, encryption where possible, intrusion detection where possible).
4. Automatic installation of Security updates and OS patches where possible. Internet facing servers will be updated at least once a quarter or if a high risk vulnerability is identified
5. Server configuration will be performed by authorized personnel only and is subject to CTO approval. This includes software installation and any other configuration.
6. Servers will be audited at least annually to help ensure compliance with industry standards.
7. Remote access will be established using encrypted protocols (TLS/SSH/RDP)
8. Disabling security controls on servers may result in disciplinary action.

13 Network Security

1. The company networking is based on a cloud infrastructure and remote access via public networks. The company assumes that employees connect to non-secure networks and protect them accordingly.
2. Network segmentation will be enforced between Dev, Staging and Production.
3. Access to internal assets is based on strong authentication or access lists.
4. Devices connected to the network will be centrally managed.
5. Traffic should be controlled and limited based on the need to work basis.

6. Communication over public networks must be established over industry standard encrypted protocols.
7. Wireless communication is used for employee workstations only. The Wireless router will be hardened and communication will be encrypted using industry standard protocols.

14 System Access Control

1. End-user Passwords
    a. Passwords must be at least 10 alphanumeric characters, uppercase, lowercase and a number or special character. Passwords must change once in 6 months.
    b. Wherever applicable, access will be based on strong authentication.
    c. Secure password storage solution will be provided to employees.
    d. Passwords must never be shared with others.
    e. Passwords must be changed if suspected of being compromised.
2. Account management
    a. All data processing systems must be password protected.
    b. Access will be based on unique user accounts and passwords.
    c. Each user will have a defined set of permissions and privileges.
    d. Where applicable, access to the system needs to be locked when not in use.
    e. Upon assignment of new user accounts, a default password shall be used. The user must be forced to change the password after the first login.

f. Administrators group and permissions must be revised twice a year to determine if all members still require such permissions.

g. The principle of least privileges required to perform a function must be used when granting permissions.

h. Default passwords will be changed promptly after product installation.

i. Access for non-company's employees, such as contractors or third parties, must be re-authorized annually.

j. Access must be promptly revoked upon employment termination.

k. If administrative passwords are known to the user, these must change.

3. Users' data access policy

   a. Users are only permitted to access data under need to work basis. Any other use of data is not permitted.

   b. Data will be stored on shared, authenticated and secure storage that was approved by the CTO.

   c. The use of external storage devices or services is prohibited. Exceptions require explicit CTO approval.

   d. Users are prohibited from capturing or obtaining passwords, encryption keys, or any other access control method, which would permit them with unauthorized access.

   e. Authorized users must not use the company systems in order to give access to other information systems to which they do not have authorized access.

   f. Users must not scan for or exploit vulnerabilities or deficiencies in the company systems or otherwise.

15 Remote Access

1. Access to the company servers and assets is remote by default, restricted to authorized sources and protected accordingly with strong passwords, multi-factor authentication and access-lists. Where possible, Single Sign On will be utilized.
2. Copying or downloading of sensitive data from servers is prohibited unless approved in writing by CTO / CSO.

16 Software Security

1. The company adheres to software vendors license agreements and copyright holder's notices. Any unauthorized or illegal use is strictly prohibited.
2. Software licensed by the company may not be sold, copied, or used for personal reasons or gain.
3. Software installation requires approval from the CTO or CSO. The vetting process will prefer known vendors on unknown ones and will consider security as part of the process.

17. R&D Security

Software developed by the company is subject to secure development life-cycle as outlined below at minimum:

1. Security will be taken into consideration as part of the product design process. Before a new system is developed or acquired, the system owner should clearly specify the applicable security requirements.
2. Code packages in use will be approved by the CTO or VP R&D, updated regularly and scanned for vulnerabilities at least annually.

3. All applications must support user authentication and permission management.
4. All user input must be validated and screened to avoid code injections.
5. Internet accessible applications will be filtered by a web-application Firewall.
6. An application vulnerability assessment will be performed on a regular basis on all internet accessible applications. Penetration test will be performed at least once a year.
7. All applications that process, transmit, or store private information must have all critical and vulnerabilities identified and corrected in a timely manner.
8. Development Change Control
    a. The company adopted an agile based development methodology.
    b. Changes are discussed and approved on a daily basis.
    c. Significant changes are documented and tracked by the feature owner.
    d. Possible impact on security is considered during the development.
    e. Version control is enforced using industry standard tools
    f. Different code branches will be managed for staging and production
    g. Access to staging areas and production will be restricted and secured with appropriate safeguards.
    h. Appropriate methods will be employed to make sure staging doesn't go into production and vice versa.
    i. All Software developed will require minimal privileges and will be tested in staging with the same permission set required for production.
    j. Any deployment of code to production will go through a review process by VP R&D or CTO.

18 Information transfer, Internet and Email Usage

This section defines the policy for maintaining the security of information transferred within an organization and with any external entity. The vast majority or information transfer is based on the Internet, Email, Instant Messaging and collaboration platforms.

1. Internet use is subject to all applicable laws, including copyright, trademarks and privacy and computer laws. In addition, Internet use is subject to the acceptable use policy.
2. Users are not permitted to post any company information to publicly or Internet accessible platforms without an explicit approval from the CTO / CEO.
3. Users are only permitted to use their own email account and collaboration platforms. The use is always subject to the policy.
4. Email is a common channel for fraud and phishing attacks; users should assume attackers are trying to lure them and demonstrate caution when using email.
5. Suspicious emails or messages over other channels should be reported to the CTO or CSO.
6. Confidential and sensitive information must be protected if sent over email and other collaboration channels.
7. Distributing SPAM or inappropriate content is prohibited.
8. Confidential Information must not be shared with any third party unless a written agreement and an NDA has been signed.

19 Suppliers, Vendors and Third Party Security

1. Any engagement with a third party supplier, provider or vendor is subject to contractual obligations and undertakings.

2. Confidential Information must not be shared with any third party unless a written agreement and an NDA has been signed.
3. Inbound access to the company systems will be granted to third parties only after approval of the CTO or CSO. Such access will be limited in time unless specified otherwise.
4. SaaS Solutions security
    a. The company uses various SaaS solutions as part of its strategy.
    b. Using a new SaaS provider requires an approval of the CTO / CSO.
    c. Any SaaS provider with access to company confidential information or assets must adhere to the following minimum requirements:
        i. Have a valid ISO27001 and/or SSAE16 SOC 2 from the past year.
        ii. Have a penetration test with no critical / high findings in the past year.
        iii. Support strong authentication.
        iv. Aligned with the GDPR and willing to sign a DPA.
        v. Support encryption of data in motion and at rest.
        vi. Will be configured by the system owner to support security best practices.

20 Physical and Environmental Security

1. Access to the company facilities is restricted to authorized personnel. Visitors escorated while on premises.
1. The doors must be kept locked at all times and opened only by authorized staff.

2. Security cameras record the office entrance and exit doors as well as communication and/or server rooms.
3. Employees carry out their duties in various locations (office, remote, public) and are responsible for information security of their own work environment and systems in use.
4. Laptops must not be left unattended in public locations and access must not be allowed to anyone besides the employee. In addition, laptops must never be left in an unattended vehicle.
5. Employees should avoid leaving company documents and assets unattended or accessible to others. In addition, hardcopies with confidential information must be properly disposed of using shredders.
6. Storage and computing devices (e.g. hard-drives) must be securely disposed of at the end of use life-cycle.
7. Production infrastructure and critical systems will be hosted only within an industry standard Infrastructure as a Service (IaaS) provider and data-centers that were approved by Security or the CTO. Such facilities are equipped with industry standard physical and environmental controls.

21. Security Incidents

1. Time is a critical component in Security Incident Response. The sooner the incident is identified, the better.
2. Employees are expected to report all suspected security incidents or vulnerabilities to the CTO or CSO via Phone, Instant Messaging or email.
3. Any attempt to prevent an employee from reporting a suspected incident or violation is prohibited.
4. Should evidence clearly indicate that a system or computer has been a victim of malicious activity or crime, the CTO and CSO will take action to perform Security

Incident Response and Forensic Analysis to assist with the incident scoping and repointing process.

5. The investigation should provide management with the following information: background, scope of issue and impact, root cause (if known at this point), suggested corrective actions and next steps.
6. Information describing all reported information security violations must be retained for a period of 2 years.

22. Malware Protection

1. All workstations must have an approved and active anti-malware software with auto updating enabled. Disabling the anti-malware protection is prohibited.
2. Server protection is based on hardening, security patches, whitelisting of outgoing traffic and intrusion detection.
3. Employees are expected to report to the CTO / CSO if a malare was detected on their workstation.

23. Backup and Restoration

1. Data stored on laptops is not backed-up by design and intentionally. Data should be stored in the approved Cloud Storage only, unless specified otherwise.
2. Production and Staging Databases are backed up daily
3. Server logs are shipped to a centralized location.
4. Source code is backed up on a daily basis
5. Restoration test for critical system components will occur once a year.

24. Monitoring

The primary purpose of Monitoring is to proactively identify potential unauthorized information-processing activities.

1. Threat monitoring tools will be enabled on critical systems and interfaces.
2. Alerts will be produced and communicated for high risk events.
3. All the actions of the users of information systems in the company are logged in order to help prevent information security incidents or deviations from the information security policy.

25. Security Awareness and Training

1. Security reminders will be sent to employees periodically and on a regular basis.
2. Employees and Contractors will undergo security awareness sessions at least once a year. The training should include the following topics: Common security risks, Acceptable use of company resources, Use of applications, tools and SaaS, Authentication protection (passwords, keys), Reporting security incidents, Privacy.

26 Software & Hardware Change Control Practices

1. IT and Production systems are subject to a formal change control procedure which ensures that only authorized changes are made. The CTO is resposbile to approve changes and any unauthorized installation or removal of hardware and software is prohibited.
2. The change control procedure must be used for changes to software, hardware and communication networks that might impact the confidentiality, integrity and/or availability of critical assets.

3. Segregation of duties: users responsible for implementing changes related to system access or such that might impact the confidentiality, integrity and/or availability of critical assets are separate from those approving such changes.

27. Management of Business Continuity

1. The company will have a well defined Business Continuity Plan for its critical systems and assets, to help reduce the risk of service and business interruption due to various causes, and allow rapid recovery.
2. Critical systems and resources will be identified, as well as the potential scenarios and mitigation strategies.
3. Generally, the company's Business Continuity Strategy is based on the fact that all critical services are hosted in top tier public cloud data-centers with redundancy and ongoing backups as well as the ability to remotely administer the environment from anywhere.

28. Adjustment

Adjustment to the requirements by law and regulatory requirements:

1. The management of the company applies the laws, standards and additional regulatory respondents that are applicable to the company.
2. The CEO of the company is responsible to verify that all employees are aware of the laws, regulations and procedures derived therefrom.
3. Identification of laws and regulations on information issues:
    - Rights of intellectual property
    - Legal evidence and records of the company
    - Right to privacy
    - Business and economic confidentiality

- Prevention of abuse of information-processing possibilities.

4. By adopting this information security system, the management of the company fulfills and implements that required by laws and standards, in aspects of information security, which it is interested and obligated to meet:
    - Information security management standards - International Standard ISO 27001
    - The Computers Law, 1995
    - Privacy Protection Law, 1981
    - Copyrights Law, 2007
    - Working according to overseas regulatory requirements.
    - European General Data Protection Regulation, 2016
    - California Consumer Privacy Act, 2018
5. A management survey detailing information security and privacy issues will be presented to a senior member of the company management to help determine the level of applicability of the policy that was adopted to the actual occurrences
6. Internal tests are executed at least once a year, in order to examine the degree of adjustment of the assistance and procedures to the organizational security policy.
7. Within the framework of the surveys and the adjustment tests, the degree of strength of the infrastructure of the information systems against hazards and malicious software will be examined.

29. Controls and auditing

All procedures shall have controls designated to assure the proper implementation. Audit trails shall be implemented across systems and shall be regularly monitored and controlled.

30. Responsibility

The CTO is responsible to apply and maintain the Policy.