DIRECTPAY

SECURITY PRINCIPLES

Change history

Version	Date	Created by	Confirmed by

Table of contents

1. Introduction

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

2. Information Security Policy

Directpay (hereinafter- company) processes confidential, personal and business (hereinafter personal and business information- sensitive information) received from customers on a daily basis. Personal information should have appropriate precautions to protect them, protect confidentiality, ensure compliance with various standards and legislation, and protect the future organization. The company undertakes to maintain the confidentiality of all its customers and protect any sensitive information about customers from third parties. Therefore, management seeks to maintain a secure environment for processing information about the company's customers so that we can fulfill these obligations.

Work with employees of confidential and sensitive information about clients should ensure:

- Limit personal use of the company information and telecommunication systems and ensure it doesn't interfere with your job performance;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defaming the reputation of the company, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personal information unless authorized;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorized software or hardware, including modems and wireless access, if you do not have agreement with the head and information security officer;
- Always leave desks clear of sensitive data and lock computer screens when unattended;

Incidents of information security should be immediately reported to the information security officer. Each of us is responsible for the fact that the information systems and data of our company are protected from unauthorized access and misuse. If you are not clear about any of the policies listed here, you should seek advice from a supervisor or an information security officer.

3. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to company established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly. The company will maintain an approved list of technologies and personnel with access as detailed in Appendix B.

- Employees are responsible for compliance with work and corporate discipline;
- Employees should ensure that they have appropriate credentials and are authenticated for the use of information systems in company;
- Employees should take all necessary steps to prevent unauthorized access to confidential and sensitive information;

- Keep passwords secure and do not share accounts;
- Authorized users are responsible for the security of their passwords and accounts;
- All PCs, laptops and workstations should be secured with a password-protected with the automatic activation feature;
- Since the information contained on portable computers is particularly vulnerable, special care should be taken;
- Postings by employees from a Company email address to newsgroups, forums and other social media, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the company, unless posting is in the course of business duties;
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan program code;

4. Disciplinary Action

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

5. Protect Stored Data

All confidential and sensitive information is stored and handled by the company and its employees must be securely protected against unauthorized use at all times. Any sensitive and personal data that is no longer required by the company for stated purposes must be deleted in a secure and irrecoverable manner, according to requirements of legislation.

6. Information Classification

Data and media containing sensitive and confidential information must always be labeled to indicate the sensitivity level:

- Confidential and personal data may include information which is protected by legal requirements and prevention of disclosure or financial penalties for disclosing such information, or data that could cause serious damage to the Company if they are disclosed or amended.
- Internal use data may include information that the data owner considers to be secure in order to prevent unauthorized disclosure;
- Public data is information that can be freely distributed.

7. Physical Security

Access to confidential and sensitive information in hard, soft and any other media format must be physically restricted in order to prevent unauthorized access to such data.

- Employees should take all necessary steps to prevent unauthorized access to confidential and sensitive information;
- A list of devices that accept sensitive data should be maintained;
  - The list should include make, model and location of the device;
  - The list should include the serial number or a unique identifier of the device;
  - The list should be updated when devices are added, removed or relocated;
- A list of employees that accept and work with sensitive data should be maintained;

- The list should include full name and surname of the employee and mobile phone number for contact; A separate list of employees which work with the personal data should be maintained. Such list should include following information:
  - Make, model, operating system (system name) and location of the device;
  - Name, surname of the employee and confidentiality classification;
  - static IP address, MAC address, antivirus and firewall;
  - Serial number or a unique identifier of the device, encryption (yes or no), auto-lock enabling (yes or no) and password protection (yes or no).

- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices;
- Personnel using the devices should be trained to report suspicious behavior and indications of tampering of the devices to the appropriate personnel;
- A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, not more than one day;
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts;
- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Visitors must always be escorted by a trusted employee when visitors are in areas that hold confidential or sensitive information;
- Employees must comply to all procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on the Company sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, not more than one day;
- Strict control is maintained over the external or internal distribution of any media containing confidential or sensitive data and has to be approved by management or information security specialist.

8. Protect Data in Transit

All sensitive and confidential data must be securely protected during physical or electronical transportation.

- If there is a necessity to send confidential and sensitive data via email or via internet or using any other methods, it should be done after authorization using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, SSL, TLS, IPSEC etc.,);
- The transportation of media containing sensitive data to another location must be authorized by management, logged and inventoried before transportation. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

9. Disposal of Stored Data

- All data must be securely disposed when data are no longer required by the Company, considering the media or application type on which it is stored, according to legislation and procedures and politics of the company;

- A permanently automatic on-line data deletion process must be applied , when on-line data are no longer required;
- Company has procedures for the destruction of hardcopy (paper) materials, which require that all hardcopy materials are shredded, incinerated or pulped so documents cannot be reconstructed;
- Company has special procedures for the electronic data and media disposal, where is stated special requirements:
    - All sensitive or confidential data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
    - If secure wipe programs are used, the process must completed concerning the industry accepted standards for secure deletion.

10. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive and confidential data demands regular training of all employees and contractors, which have access to sensitive and confidential information of company.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A)
- Company security policies must be reviewed annually and updated as needed.

11. Network Security

- Firewalls must be implemented at each internet connection and any demilitarized zone and the internal company network.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the sensitive data environment.
- Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- All inbound and outbound traffic must be restricted to level which is required for the confidential and sensitive data environment.
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented.
- All outbound traffic has to be authorized by management (i.e. what are the whitelisted category of sites that can be visited by the employees) and the restrictions have to be documented.
- The company will have firewalls between any wireless networks and sensitive data environment.
- The company controls the wireless network using authentication methods through a e-token with a password on the certificate and access permission.

- A topology of the firewall environment has to be documented and has to be updated in accordance with changes in the network.
- No direct connections from Internet to sensitive data environment will be permitted. All traffic has to traverse through the firewall.

12. System and Password Policy

All users, including contractors and vendors with access to the Company's' systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords:

- System configurations must include common security parameter settings;
- All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into the Company network and all unnecessary services and user/system accounts have to be disabled;
- All unnecessary default accounts must be removed or disabled before installing a system on the network;
- All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed;
- All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.
- Any insecure protocols, daemons, services in use must be documented and justified;
- All users must use the password to access the company network or any other electronic resources;
- All user ID's for terminated users must be deactivated or removed immediately;
- The User ID will be locked out if there are more than 15 unsuccessful attempts enter password for password to connect on information systems of company. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled until the information security officer enables the account.
- All system and user level passwords must be changed at least after six months;
- A minimum password history of three must be implemented;
- A unique password must be setup for new users and the users are obligated to change the password on login first time;
- System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands;
- Administrator access to web based management interfaces is encrypted using strong cryptography.
- Users' responsibility is to select a password that is hard to guess;. A strong password must:
    - Be as long as possible (never shorter than 8 characters);
    - Include mixed-case letters, if possible;
    - Include digits and punctuation marks, if possible;
    - Not be based on any personal information;
    - Not be based on any dictionary word, in any language.
    - Password history is set to 3 and password expiry warning period is set to 90 days

13. Anti-virus policy

- All machines must be configured to run the latest anti-virus software as approved by the Company. The preferred application to use is Kaspersky or ESET NOD Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use should be detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits).
- All removable media (for example floppy and others) should be scanned for viruses before being used.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans.
- End users must not be able to modify any settings or alter the antivirus software.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.
- E-mail with attached files received from suspicious or unknown sources should not be opened. All such e-mails and their investments should be notified to the information security specialist and follow his instructions.

14. Patch Management

- All workstations, servers, software, system components etc. owned by the Company must have installed up-to-date system security patches to protect the information from known vulnerabilities.
- Wherever possible, all systems and software’s must have automatic updates for system patches issued by their respective suppliers. Security patches must be installed within one month from the date of release by the relevant supplier.
- Any exceptions to this process have to be documented.

15. Remote Access Policy

- All hosts connected to internal networks of the Company using remote access technologies will be regularly monitored.
- Vendor accounts that have access to the Company's network will be opened only for the period of time that access is required and will be disabled or deleted after access is no longer required.

16. Vulnerability Management

- To all the vulnerabilities would be assigned a risk rankings-High, Medium and Low based on industry best practices such as CVSS base score.

17. Configuration standards

- All network device configurations must adhere to the Company required standards. Using this guide, a boilerplate configuration has been created that will be applied to all network devices before being placed on the network.
- Before deployment to production, the system must be inventoried in accordance with the applicable configuration standard.
- Updates to the operating system and/or configuration parameters of network devices that fall under the Company's standards are announced by the Information Security Department. Updates should be applied within the time period specified by the Information Security Department.
- Administrators of network devices that do not adhere to the Company standards (as identified via a previous exception) must document and follow a review process of announced vendor updates to operating system and/or configuration settings.
- All configurations of network devices are checked by the Zabbix warning and monitoring system, with the appropriate configuration change notification, responsible employees.
- Where possible, network configuration management software will be used to automate the process of confirming adherence to the boilerplate configuration.
- All inconsistencies will be evaluated and corrected by the Office Support Division or UNIX Division.

18. Change Control Process

- Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored (Zabbix or other software).
- All requests for changing the software or hardware configuration must be registered in the servicedesk or helpdesk system regardless of whether they are approved or rejected in the central Teamwox system. The approval of all change requests and their results must be documented. A documented audit trail maintained at the business unit level containing the relevant information must be maintained at any time. This should include documentation for the change request, permission to change and the outcome of the change. No person should be able to make changes to production information systems without the approval of other authorized personnel.
- A risk assessment shall be performed for all changes and dependent on the outcome, an impact assessment should be performed.
- The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

- Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimize the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.
- Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.
- All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorized user, the impact assessment was performed and proposed changes were tested.
- All changes made by the user must be described in the servicedesk section where these changes were agreed.
- The procedures for undoing and restoring after unsuccessful changes should be described. If the result of the change differs from the expected result (as indicated when testing the change), should be noted procedures and responsibilities for the restoration and continuity of the affected areas. Recovery procedures will be restored so that systems can return to what was before the implementation of the changes.
- Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed.

19. Audit and Log review

- This procedure covers all logs created for systems in a confidential data environment based on the customer data stream in the Company's network, including the following components:
    - Operating System Logs (Event Logs).
    - Firewalls & Network Switch Logs.
    - Logs of information systems of the company processing data of clients.
    - Logs of Zabbix monitoring system.
- The review of journals should be conducted using the Zabbix network monitoring system, which is controlled from the Zabbix Company web console.
- The following personnel are only people who are allowed access to log files:
    - Information Security Officers;
    - Those who are approved of such access after agreeing with an information security officer and the head of the department.
- The Zabbix network monitoring software is configured to alert employees in the office support department and information security department employees to any conditions that are believed to be potentially suspicious for further investigation.
- Alerts about incidents come both by e-mail and by SMS to contact numbers of company employees. The notice contains only a brief description understandable to the employee.
- The following operating system events are configured for logging:
    - Any additions, modifications or deletions of user accounts;
    - Any unsuccessful or unauthorized attempt to log into the system;
    - Any modification to critical system files;
    - Actions taken by any individual with root or administrative privileges.
- The following database system events are configured for logging and monitored by the network monitoring system:
    - Any failed user access attempts to log in to the database;
    - Any login that has been added or removed as a database user to a database;
    - Any login that has been added or removed from a role;
    - Any database that has been created, altered, or dropped;
    - Any database object, such as a schema, that has been connected to;

    - Actions taken by any individual with DBA privileges.
- Any actions on sensitive data in Information systems logged.
- Any unauthorized attempts to authenticate a user in the information system or on any device such as:
    - Authenticate in Information System
    - Authenticate in VPN service company

- IT audit will be is provided in accordance with the best practice of ISO 27001.

20. Penetration testing methodology

- In this section should be listed the risks inherent in conducting penetration testing over the information systems of the company. Additionally, it should be noted for each mitigation measures that will be taken. Examples might be:

Example 1

Risk: Denial of Service in systems or network devices because of the network scans.

Mitigation measure 1: network scans must be performed in a controlled manner. The start and end of the scan must be notified to responsible personnel to allow monitoring during testing. For any sign of trouble will abort the scan in progress.

Mitigation measure 2: scanning tools must be configured to guarantee that the volume of sent packets or sessions established per minute does not cause a problem for network elements. In this sense, we must perform the first scans in a very controlled way and a use minimum configuration that may be expanded when is evident that the configuration is not dangerous for network devices or servers in the organization.

- If an incident occurs during the execution of the tests that have an impact on the systems or services of the organization, the incident should be brought immediately to the attention of those responsible for incident management in the project
- For all findings or vulnerabilities identified during the tests carried out will be generated and documented sufficient evidence to prove the existence of the same. The format of the evidence can be variable in each case, screen capture, raw output of security tools, photographs, paper documents, etc.
- As a result of tests performed should generate a document containing at least the following sections:
    - Introduction;
    - Executive Summary;
    - Identified vulnerabilities;
    - Recommendations for correcting vulnerabilities;
    - Conclusions;
    - Conclusions;
    - Evidence.

21. User Access Management

- Access to company is controlled through a formal user registration process beginning with a formal notification from HR or from a head of department in his servicedesk.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.

- There is a standard access level; other services may be available if they are specifically authorized by the Head of the department and an information security officer.
- The request for access is written by the employee's manager in the corresponding branch of the servicedesk and coordinated by the information security officer. The request should include:
    - Full name of the employee who needs access to the information systems of the company;
    - Information system;
    - List of necessary rights;
    - Time to access.
- Access to all company systems is provided by Information security specialist and can only be started after proper procedures are completed.
- Access to all systems of the company is provided by an information security specialist and can be launched only after obtaining the appropriate approval of an information security officer.
- As soon as an individual leaves the Company, all his / her system logons must be immediately revoked.
- As part of the process of termination of the employment contract, HR (Head of the department where the employee worked) will inform the information security specialists of all graduates and the date of their departure.
- User access right review should be performed at least every 6 month for each information system and evidence is kept for audit trail.

22. Access Control Policy

- Access Control systems and approval system are in place to protect the interests of all users of The Company computer systems by providing a safe, secure and readily accessible environment in which to work.
- The Company will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.
- The distribution of rights to privileges (for example, a local administrator, a domain administrator, super user, root access) is limited and controlled, and permission is provided jointly by the information security department and the Office support department. Technical teams must protect against issuing privileged rights to all teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Access to IT resources and company services is provided only with a reliable a strong password from this device, known only to the employee who was released by this device.
- Access to confidential, limited and protected information will be limited to the information security officer. Requests for permission to access, modify or revoke.
- Users are expected to become familiar with and abide by The Company policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.

Appendix A

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the Company by third parties such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with the Company, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorized to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the Company security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

Employee Name

_____

Department

Appendix B

List of agreed software for use

Software Name	Description	Approved User
Kaspersky EndPoint Security	Anti-virus software	All employed staff
TrueCrypt	Software for Create an encrypted logical (virtual) disk with sensitive data(if needed), which is stored as a file. Also fully encrypted a partition of a hard disk or other storage medium, such as a floppy disk or USB flash drive. All saved data in the TrueCrypt volume is fully encrypted, including file and directory names.	All employed staff