2014

WorldEscrow N.V./S.A.

SECURITY POLICIES AND PROCEDURES

This document describes internal security rules within the WorldEscrow N.V./S.A. organization.

Content

1) Employee Responsibilities

i) All employees and authorized external parties to include but not limited to contingent workers, suppliers and business partners must be aware of their responsibilities to protect WorldEscrow information assets.

ii) Employees and authorized external parties who identify, label, handle or dispose of WorldEscrow information assets must comply with the requirements of the Protection of Information Assets standard.

protection-informatio
n-assets-594.pdf

2) Use and Disclosure of Information

i) Employees and authorized external parties must use WorldEscrow information assets only for business purposes, internally or externally, based on business need and will take appropriate precautions to prevent unauthorized and unintentional disclosure of information assets. Appropriate precautions include but are not limited to: not discussing sensitive WorldEscrow business in public, only sharing information assets with authorized individuals with a business need to know, and properly disposing of information assets that are no longer needed.

3) Disclosure

i) Disclosure includes both written and verbal communication, by means of all channels, including e-mail, internet and social media, (for example, Facebook, Twitter, Linkedin).

ii) WorldEscrow internal disclosures of sensitive information may be provided to people within WorldEscrow only for valid business purposes.

iii) WorldEscrow external disclosures of sensitive information may be provided to a customer, channel partner, supplier, other business partner or anyone else outside WorldEscrow only when business needs to require WorldEscrow to make such a disclosure. The identity of the receiving party needs to be verified and an authorized Confidential Disclosure Agreement (CDA) executed by the receiving party – see Non disclosure_WE_EN.pdf.

iv) Confidential Disclosure Agreements (CDAs) are designed for use in situations where it becomes necessary for WorldEscrow to disclose confidential information to, or receive confidential information from, someone outside WorldEscrow (the “software suppliers”).

v) This Agreement should be used if it becomes necessary for WorldEscrow to disclose confidential information (such as product design) to anyone outside WorldEscrow.

vi) It is the responsibility of every employee and authorized external party to understand WorldEscrow's policy with respect to the receipt or disclosure of sensitive information and to know the basics of when and how to use a CDA appropriately.

4) WorldEscrow labels

i) WorldEscrow information assets must be identified, handled, labeled, and disposed of in accordance with the sensitivity of the content, as defined by WorldEscrow policies and procedures, available at: Protecting WorldEscrow 's Information Assets.

ii) WorldEscrow's Labels are:
WorldEscrow Confidential is the label for any information that is to be restricted within WorldEscrow to only those internal parties receiving the information with a “need to know". Information that is labeled WorldEscrow Confidential must be properly protected to avoid unauthorized access to the information and will only be posted on the Intranet or internet if it is password protected or otherwise placed in a way (that is, encryption) that it cannot readily be accessed by unauthorized parties.

WorldEscrow sensitive information labeled as Private will be safeguarded through secure communications and authentication in the case of electronically posted information.

Recycling of hardcopy sensitive information is not an acceptable form of disposal unless the sensitive information is crosscut according to the specifications above prior to recycling.

5) Digital Media

i) All digital media must be securely erased electronically by overwriting or physically destroyed prior to disposal or reassignment of the system.

ii) The following media types are used in process of the escrow depositing : CD, DVD, USB stick, external drive, HD, ftp. For the ftp the zip, tar file is encrypted or password protected.

iii) WorldEscrow always recommends to use the encryption to transmit the data. The public PGP key is available on the website www.worldescrowdeposits.biz in order to encrypt the escrow deposit.

6) Depositing via online depositing system

i) Once, the escrow material has been deposited via ftp.worldescrowdeposits.biz. On the server runs an application that's checking constantly vulnerability of the system. Once the deposit is transmitted it is registered in our system and the deposit is moved to the external drive password protected. In some cases when required by the contract, the escrow deposit which arrived via the ftp system is written to CD/DVD. Deposits are located at the local vault (=locked) till the moment the escrow material is verified. Once the escrow material is verified it is immediately deposited at the secure vault at the bank.

7) Deposits arriving via email

i) In certain situation when the volume of the escrow deposit is very small it can arrive via email as compressed file (Zip, Rar, tar…) and password protected or encrypted. Once the deposit with the escrow material has arrived via the email it is registered in our system and moved to the external drive password protected. Further the same procedure is followed as described above in the chapter §6.

8) Security Processes for Handling and Disposing of Sensitive Information

i) Processes must be implemented to safeguard WorldEscrow sensitive information and waste throughout the collection and disposal process as agreed in escrow agreement. WorldEscrow employees who handle sensitive information are responsible for disposing of sensitive information in a manner that prevents unauthorized disclosure of the material.

ii) Sensitive material containers are to be made available to employees so they may deposit sensitive waste for disposal.

iii) Keys (or combinations) are issued on the regular basis only by 2 people authorized people within the company who are authorized to collect sensitive material.
iv) Sensitive information is not allowed to be left in a state or position where it can be accessed without detection by unauthorized individuals.

9) Supplier security requirements

i) Access points are monitored electronically.
ii) The access points are capable of monitoring normal and after- business hours the access and ensure there are no unauthorized employees or visitors entering the supplier's facility.

10) Supplier documented security procedures

i) Security incidents (including theft or attempted thefts) concerning sensitive information waste must be reported to WorldEscrow as soon as possible.
ii) Knowledge of WorldEscrow sensitive information being onsite is restricted only to persons with a need to know, and any exception requires WorldEscrow approval.
iii) Keys, and locks are controlled in areas where WorldEscrow 's sensitive information is stored.
iv) Any deviations, discrepancies, suspicious events, or the discovery of inappropriate materials must be reported to the WorldEscrow Managing Director.
v) Employee termination procedures must be in place to ensure the return of IDs, access cards, keys, and other sensitive information.
vi) During the disposal process, it may be necessary to temporarily store sensitive information until it can be further transported or destroyed.
vii) Sensitive information is stored in a dedicated, secured location: secure vault of the bank, the locked container or safe.
viii) Access to sensitive material storage areas is to be restricted solely to authorized workers engaged in the sensitive material disposal process.
ix) Sensitive material must not be left unsecured or unattended during the transportation process.
x) Sensitive material must be destroyed in such a manner as to render it unusable to unauthorized persons.
xi) Acceptable methods must be used for destruction of paper documents and CD’s/DVD’s like shredding devices.
xii) Sensitive material may only be recycled after it has been destroyed and is unreadable.

11) Securing Sensitive Information

i) A copy of the full deposit, including reporting history are to be securely kept in a local secure vault at another geographical location. This to guarantee continuity of WorldEscrow service, which is: to help and safeguard the continuity of business operation. This in case WorldEscrow not might be in a position to continue its escrow activities anymore.
ii) Sensitive information, hardcopy or electronic, must be properly secured and stored to prevent unauthorized access at unattended desks, home offices, or mobile equipment.
iii) Laptops are theft targets when left in vehicles, and employees should refrain from leaving equipment in vehicles.
iv) Removable digital media such as USB drives, external drives and printed reports are to be controlled and secured if workspace is unattended.

12) Special Events

i) Sensitive material identification and markings are to be used for event handouts, printed material, visual projections and other presentation material.
ii) Unwanted information assets must be controlled and secured until they can be disposed of as required by this standard.
iii) All information assets are to be removed from conference rooms after meetings by the host.
iv) Whiteboards are to be erased.
v) Flip chart papers are to be destroyed.
vi) Mobile phones are to be turned off during sensitive meetings to prevent unintended transmissions.
vii) Avoid discussing or working on sensitive information in common areas.
viii) When traveling, maintain visual control of mobile equipment.

13) Security rules for hardware components

i) Physically secure your PCs, laptop, USB memory devices by using credentials at least 8 characters string with one capital letter and at least one number in between.
ii) Desktops/laptops must be securely protected by anti-virus software.
iii) Run at least once a week an anti-malware software on your desktop/laptop.
iv) Do not download suspicious or unapproved software from unfamiliar websites.
v) Allow automatic updates and protect sensitive information in all forms (electronic, hardcopy, intellectual).
vi) The window session must be locked in case the employee leaves the computer.
vii) Server area must be securely protected with high level of passwords protection minimum 10 alphanumeric character combination.
viii) The passwords need for the desktops and laptops must be changed on a regular basis at least 2 times a year. The servers passwords are to be restricted only to the server administrator.

14) Secure keys management

i) Encryption keys are generated by OpenPGP software.
ii) The key pair (public and private) and fingerprint generation happens at least once a year with the limited timestamp (until date) and appointed to 2 people of WorldEscrow NV.
iii) Each time the key pair is generated the private key and the fingerprint is deposited at the secure vault at the bank.
iv) The key pair is embedded in a certificate singed by a common known CA as implicit proof of authenticity.
v) Only two WorldEscrow employees are assigned to the key pair and are both registered in CA for validation via http://www.cacert.org/.
vi) In case of any doubt (example: MITM attack is suspected….etc) the public key fingerprint can be sent via mobile or via the usual post as a hardcopy in order to proof the authenticity of the PGP key.
vii) No internet connection is used on the dedicated computer during the decryption process.
viii) FTP login credentials are created randomly by the DirectAdmin on the ftp server.
ix) The credentials on the ftp server are being changed for every deposit.