CBA Information Security Policy

1 General

1.1 Subject

This security policy involves the security of Comprehensive Benefits of America, LLC. It consists of security objectives, guidelines for their achievement, and overall security management strategy and implementation of policies on key security mechanisms. Information security policy complies with EVS-ISO/IEC TR 13335 Guidelines, models and terms, the standards EVS ISO / IEC 2382-8 and EVS-ISO/IEC TR 13335 are used for information security terms.

1.2 Scope

The security policy is for all subdivisions of CBA and regulates interactions and relationships with the following subjects:

partners, customers and subcontractors

state agencies

media and public

1.3 Goal of security policy

The security policy establishes the guidelines and procedures in the scope of assets that CBA employees are required to know and comply with as a primary means of achieving security goals. Security policy is the base for planning, design, execution and management of security.

1.4 Security Objectives

1.4.1 Security of assets must be maintained to the extent that CBA could function normally and without interruptions in the case of most probable threats, to achieve its business goals.

1.4.2 Security measures must be economically justified and their disruptive effect to CBA operations and staff must be as small as possible.

1.4.3 Asset availability, integrity and confidentiality must conform to an average level of security.

1.4.4 Compilance to the security legislation (including copyright, personal information, state laws and regulations and workers health and safety requirements and fire safety requirements) must be ensured. To meet this requirement, some objects and processes must be protected with measures above the average level of security if needed.

1.4.5 Due to contractual and similar relationships with partners, security measures above the average level must be used to meet the requirements of objects and processes where appropriate. When preparing the contracts, resource costs for additional security must be taken into accound and the security measures must be economically justified.

1.5 Principles of security

1.5.1 General security methodolgy is based on the standards EVS-ISO/IEC 27001 and EVS-ISO/IEC 17799.

1.5.2 The basline for electing, deployment and management of security measures is ISKE that is compiled from German Information Security Agency's (BSI) baseline security. The term 'secure' in the following text means the compliance to ISKE baseline security measures.

1.5.3 Assets usage permissions are granted to the workers on the basis of work-related needs.

1.5.4 For any asset the is some individual responsible for it.

2 SECURITY ORGANIZATION AND INFRASTRUCTURE

2.1 Security Council

2.1.1 Security Council makes the important decisions on the subject of security. Security Council consists of CBA chairman of the board and the people in the following roles:

chief security officer

information security officer

network security officer

2.1.2 Security Council shall meet at least once a year to examine the security situation and to make necessary changes to security practices.

2.1.3 Security Council members are determined by the executive management.

2.2 Responsibilities

2.2.1 Security officers responsibility is determined by the subdivision or area they work in.

2.2.2 CBA chief security officer is responsible for the general security in CBA.

2.2.3 Telephone Communications security is the responsibility of telephone specialist.

2.2.4 People are responsible for assets given to them for work.

2.2.5 People are financially responsible.

2.3 Temporary replacement of the responsible persons

2.3.1 Security roles listed in section 2.1 must be filled all the time. Efforts should be made to avoid the simultaneous missing of a role holder and his deputy. When this is not possible, security officer will appoint another deputy for the corresponding period of temporary absence, and instruct him.

2.3.2 Information security officer will be responsible for the security of assets that are in use by staff members without continuous security role.

2.4 Notification of incidents

2.4.1 All real and alleged security incidents must be reported immediately.

2.4.2 Information security incidents must be reported to subdivisions information security officer.

2.4.3 General security incidents must be reported, depending on the situation, either to department head and / or to a local or general security officer, or to immediately contact the appropriate authorities (see 8.4).

2.5 Additional security policies

Subunits have the right to impose additional provisions and detailed policies about its objects and security mechanisms, if these are not inconsistent with this security policy.

3 RISK ASSESSMENT AND RISK MANAGEMENT

3.1 Acceptable residual risk

3.1.1 Acceptable residual risk is decided once a year.

3.1.2 CBA board accepts the residual risk of $250,000 for 2020.

3.2 Testing of security conformance

3.2.1 Security Council member test the conformance of security to the security policy at random at least once a month.

3.2.2 Security Council performs an internal audit to check the conformance to baseline security at least once a year.

3.2.3 External audit is perfomed when necessary, but not less frequently than once every three years.

3.3 Insurance

3.3.1 Under the present conditions, insurance is not economically justified for CBA.

4 PHYSICAL AND INFORMATION ASSETS

4.1 Critical Assets

This security policy is mainly targeted at the security of assets listed in this section.

4.1.1 Infrastructure

The following items must meet the medium level of availabilty and integrity:

premises

technical infrastructure, power distribution and other general purpose utility systems

equipment and tools used for maintenance, catering and other support activities in the premises

outside territory, car park cars

4.1.2 Data anddocumentation

For CBA's activity, especially the following types of data are important security-wise:

4.1.2.1 Business data with medium confidentiality: strategic development plan, contracts, product development plans and similar information the disclosure of which could reasonably affect the normal functioning and competitiveness of CBA.

4.1.2.2 Business data with higher confidentiality requirements: business information covered with state secret or confidentiality agreement or confidentiality requirements of other agreements.

4.1.2.3 Self-produced data for which the integrity and availability are essential: the intermediate and final results of internal development, including self-made software.

4.1.2.4 Self-produced data for which the confidentiality is important: input, intermaediate and result data covered with state secret or confidentiality agreement.

4.1.2.5 Personnel data which is confidential: including files about workers, contracts, record books, payroll data, health data.

4.1.2.6 Process management data with confidentiality requirements: detailed work plans and worker assignments and administrative data about security mechanisms.

4.1.2.7 Auxiliary data that needs availabilty and integrity: management data about infrastructure, documentation for equipment and infrastructure, professional literature.

4.1.3 Hardware

The integrity and availability of the following hardware is important:

servers

workstations

notebooks

network infrastructure equipment

Peripherals are counted to belong with computers.

4.1.4 Communications systems

Availability and integrity of the following communications equipment is important:

PBX (telephone exchange)

phone cabling and distribution devices

telephones, including mobile phones

firewalls, routers, modems, wireless networking and other data communications equipment

communication cabling

4.1.5 Software

Availability, integrity and legality of commercial and self-made software is important.

4.1.5.1 The developed special software (see also 4.1.2.3, 4.1.2.4). Contains the software for companys own purposes. Source code of self-made software is confidential, unless decided otherwise. Self-made software should be be under copyright protection.

4.1.5.2 Purchased special software.

4.1.5.3 Purchased general-purpose software:

Microsoft Windows 7 Professional

Microsoft Windows 10 Professional

4.1.5.4 Obtain freeware only from trusted sources, and in agreement with the head of IT.

4.1.6 Materials

To ensure the availability of equipment and continuity of processes, there must be a 5 working day supply of the following materials:

paper

printer toner

floppy discs

CD blanks

DVD blanks

magnetic tapes

USB memory sticks

4.1.7 Other assets

Availability and integrity is important for the following resources:

lab equipment

component products and semi-finished products

office equipment (copiers, binding machines etc.)

furniture

4.2 Asset accounting

4.2.1 Information assets listed in Section 4.1, except those of (4.1.6) and the complimentary property (4.1.5.4) must be identified, documented, evaluated quantitatively or qualitatively, and listed in asset specifications according to ISKE requirements.

4.2.2 In assessing the price of assets, both monetary value of assets and possible indirect damages from security incidents (destruction, damage, exposure) resulting in the slowdown in work processes, damage to public image etc, must be taken into account.

5 RISKS AND WEAKNESSES

Forplanning, implementation and management of security, the following risks will be considered typical, and security measures should be based on this selection.

5.1 Spontaneous risks

Fire

Thunderstorm

Water and fire extinquishing damages, including stormwater, emergency pipelines, etc.

Human error

Fluctuations in power quality and plain blackout

Hardware error

Interruption of external communications

Loss of staff

5.2 Attacks

Theft

Viruses

Penetration into the internal network from public network

Distributed Denial of Service (DDoS)

Sniffing of an internal computer network

Interception of oral communication

Workers' deliberate security breaching behavior, internal attacks

6 SECURITY MEASURE POLICIES

The implementation and management of basic security mechanisms must comply with the following policies and guidelines.

6.1 Access policy

6.1.1 Access to resources is role-based, according to job requirements.

6.1.2 IT user roles are defined by IT system features and from the structure of IT management.

6.1.3 IT roleset must have at least 3 levels for access to data: no acces, read-only, read-write.

6.2 Password management

6.2.1 Access passwords must be changed at least twice a year.

6.2.2 System, network and other administrative passwords must be stored in written form in a safe.

6.3 Cryptography policy

6.3.1 For accessing internal network resources across the public network and for the transmission of confidential data across public network, only secure connections must be used: VPN connections, SSL / HTTPS connections, and encrypted mail messages.

6.3.2 All confidential data on computers being carried outside the company perimeter (laptops, computers of home workers), all confidential data on hard disks must be encrypted. Encryption keys must be duplicated in a safe backup.

6.3.3 The minimum acceptable key length for symmetric encryption is 256 bits.

6.3.4 Minimaalne lubatav võtme pikkus asümmeetrilise krüptosüsteemi kasutamisel on 1024 bitti. 6.3.4 The minimum acceptable key length of asymmetric encryption is 1024 bits.

6.4 Logging and log reviewing policy

6.4.1 Logs to must be able to identify authorized and unauthorized attempts to access recourses, with the exact time and place of origin.

6.4.2 System and networking log check must be performed

randomly at least once a week

after the respective incidents.

6.4.3 All logs must be stored for at least four weeks.

6.5 Removal policy

6.5.1 All unnecessary paper documents with confidential data (see 4.1.2.1-4.1.2.6) must be destroyed with a shredder.

6.5.2 Retired and / or discarded from archive storage media must be destroyed physically.

6.5.3 To delete state secret or highly confidential data from disk, secure deletion must be used.

6.6 Work environment

6.6.1 New software must be tested before use and confirmed to be suitable.

6.6.2 No real data must be used for testing and demos.

6.7 Legality policy

6.7.1 All assets must be acquired legally.

6.7.1 All uses of the assets should be legal.

7 SECURITY OF COMMUNICATION

7.1 Networking infrastructure

7.1.1 CBA network must meet the following two-level logical structure:

External network outside the firewall

Internal network inside the firewall

7.1.2 All cabling (electricity, communications, telephone, alarm system, etc.) must be marked and documented and placed hidden.Wiring documentation must include the exact location in the building, cable specifications (make, capacity), wire marking (color, symbols, markings in distribution points etc.), the location, type, installation and repair times of distribution equipment and type of cables.

7.2 Internal network management

7.2.1 The company has one common internal network.

7.3 Servers

7.3.1 Internal and external web servers must be located in different computers.

7.3.2 In addition to the web serving, external web servers can only run FTP server.

7.3.3 Mail server relay feature must be absent or permanently disabled.

7.4 E-mail

7.4.1 Internal e-mails should not be sent outside internal network (even in quoted form).

7.4.2 Mail sent to public network must include the proper name of the sender.

7.4.3 Incoming and outgoing mail must be subjected to virus scanning.

7.4.4 Opeing active contents (.EXE, .VBS etc.) in incoming e-mail is permitted only for security investigation purposes and in agreement with information security officer.

7.4.5 When possible, avoid sending documents in formats allowing macros.

7.4.6 Files attached to e-mail must not contain parts of other files which do not show up with the viewer.

7.5 Phone calls

7.5.1 Transmission of confidential information by telephone should be avoided, especially with mobile phones.

7.6 Fax

7.6.1 CBA's fax may be used only by authorized personnel.

7.6.2 Fax modems of LAN workstations must not be connected to external networks.

7.7 Exchange of data using removable media

7.7.1 Materials transferred using portable storage device or a CD must not contain any hidden data or other materials.

7.7.2 When receiving materials with portable storage device, virus check must be performed.

7.7.3 Equipment to be delivered must not contain extraneous programs or data.

7.8 Oral communication

7.8.1 Avoid confidential matters in public zones.

8 GENERAL SECURITY

8.1 Security of perimeter and zones

8.1.1 Doors

8.1.1.1 Corridor doors must be self-closing and self-locking.

8.1.1.2 The entrance to building must be locked outside of working hours.

8.1.2 Access to premises

8.1.2.1 Permanent employees are permitted access to the main entrance during working hours, and, as appropriate, to the premises of their workspace as their role needs. Entrance at any other time is governed by the internal rules.

8.1.2.2 The right to access to other premises will be given when appropriate, but only during working time.

8.1.3 Other locks

8.1.3.1 Spare keys to all rooms must be kept in locked fireproof cabinets.

8.1.4 Windows

8.1.4.1 All windows must be securely closable.

8.1.4.2 Window must be watertight enough to prevent rain damage.

8.1.4.3 Rooms with windows on the groundfloor must be equipped with security alarm sensors and secure window frames.

8.1.5 Guard

8.1.5.1 During working hours, CBA will ensure security. At night and on public holidays, a security company will provide security.

8.1.6 Security alarm system

8.1.6.1 Windows: See 8.1.4.3.

8.1.6.2 Essential rooms must contain security sensors, preferably motion sensors and door opening sensors too.

8.1.6.3 Alarm system is activated and deactivated manually by employees.

8.1.6.4 Alarms are automatically transferred to the security company.

8.1.6.5 Alarm system must be tested on alarm, and at random during other times.

8.1.7 Visitors

8.1.7.1 Visitors are allowed in the building of CBA only when accompanied by an attendant.

8.1.7.2 Attendant will meet the visitor at the entrance.

8.1.7.3 Meetings, seminars and other events where any other parties are involved should take place only in meeting rooms.

8.2 Safety of rooms

8.2.1 Room designation

8.2.1.1 Server rooms, archive rooms and technical rooms must not have generally understandable labels and should not appear in building guides.

8.2.2 Fire alarm system

8.2.2.1 Fire alarm sensors must be installed according to manufacturer's and fire protection rules' requirements.

8.2.3 Fire-fighting equipment

8.2.3.1 The number of fire extinguishers, layout and verification must comply with fire regulations.

8.2.3.2 The fire extinguishers in rooms with computers or electricity distribution must be gas or powder based.

8.2.3.3 Staff should be instructed to use fire extinguishers.

8.2.4 Environmental measures

8.2.4.1 The server room must have air conditioning, which regulates air temperature and humidity.

8.2.5 Security of premises

8.2.5.1When levaing worplace, the workers must close the windows and lock the door if it is lockable.

8.2.6 Security of special rooms

8.2.6.1 Server rooms must have security-enhanced construction, they must be equipped with a security and fire alarms and gas based fire extinguishers. Server room must be permanently locked.It is advisable to double the floor to prevent water damage.

8.2.6.2 Heating system control rooms must be permanently locked.

8.2.6.3 Electricity distribution rooms must be equipped with fire alarms and extinguisher, and locked up.

8.2.6.4 Electricity distribution boards must be securely locked.

8.2.6.5 PBX room must be equipped with security alarm and permanently locked.

8.2.7 Workplace security

8.2.7.1 It is recommended that all workplaces comply with the principle of an empty table, ie.when leaving the room after work, remove all the documents and media from table and from other visible locations, and always lock your computer screen.

8.2.7.2 Important documents and media (see 4.1.2.1-4.1.2.6) and small but valued physical assets must be kept in a locked cabinet or drawer.

8.2.8 Maintenance and repair work

8.2.8.1 External maintenance and repair personnel is allowed to the premises only when accompanied by an attendant.

8.2.8.2 At the any given time, only the minimum required number of rooms must be opened for maintenance and repair.

8.2.8.3 Keys or other access devices must not be given to the repair workers.

8.3 Physical security of equipment

8.3.1 Mobile equipment

8.3.1.1 Users of cell phones and laptop computers are responsible for their security.

8.3.2 Other devices

8.3.2.1 Non-mobile equipment may be taken out of CBA building only with the permission of department head or the directorate.

8.3.2.2 In unsafe locations (such as exhibitions and trade fairs), to use equipment safely, use some means to fasten the equipment to the table - for example, laptop security locks.

8.3.3 Storage

8.3.3.1 CDs, DVDs, tapes, etc. must be labeled.

8.3.3.2 Archive, backup and other media must be kept in special cabinets.

8.3.4 Interruptions in technical services

8.3.4.1 Server backup power for at least 5 minutes must be provided using UPSes.

8.3.4.2 Alarm system must have an emergency power supply with batteries for at least 48 hours.

8.3.4.3 PBX must have backup power for at least two hours, using batteries.

8.4 Communication with the authorities in case of security incident

8.4.1, The employee who discoveres the danger will contact police or emergency number 911.

8.4.2 Communication specialist will deal with network service provders.

8.4.3 On electricity issues, security officer interacts with the relevant authorities.

9 PERSONNEL SECURITY

9.1 Staff selection

9.1.1 Candidates for vacant jobs should be selected on the basis of job requirements.

9.1.2 Each candidate's background must be checked from a security risk perspective.

9.2 Procedures for appointment

9.2.1 On appointing to the job, new staff must carefully read the following documents and confirm their knowledge with their signature:

contract

job description

security guide

CBA security policy

internal rules of procedure

9.2.2 For contract workers, the appropriate security requirements must be included the contract in each case.

9.2.3 Head of department is responsible for instructing of a new employee.

9.3 Notification

9.3.1 Staff will receive notifications via the intranet news.

9.3.2 Operative security information is distributed through the inner mailing list.In this mailing list the follwing events must be announced:

security incidents

security environment changes

recruitment and dismissal

changes and additions to the internal network security system

9.4 Training

Staff security training consists mainly of

reading the security guides

consultancy with subunits information security officer

9.5 Procedures for dismissal

9.5.1 By the end of the last working day, the dismissed worker must give all of its assets back to CBA.Department head is responsible for the take-back.

9.5.2 By the end of the last working day, all means of access (keys) and credentials must be taken away (change the passwords, remove from access control lists).Department head is responsible for the take-back, but department's information security officer will do it.

9.5.3 If necessary, the measures in 9.5.1 and 9.5.2 are taken immediately after dismissal decision.

9.6 Penalties

9.6.1 In case of breach of security requirements, the offender will be proesecuted with penalties ranging from public reprimand to dismissal.

9.6.2 CBA directorate must make the offender to compensate caused physical damage.

9.7 Telework

9.7.1 Teleworking is entitled case by case.

9.7.2 Teleworking may be conducted only through a secure communications and in compliance with other appropriate security requirements.

9.8 Access rights compliance testing

9.8.1 User access rights' compliance with the real needs shall be inspected at least twice a year.

9.9 Staff contacts

9.9.1 Workplace and home contacts of each worker of CBA must be available to all employees on the intranet.Contact details are confidential.

9.9.2 External web site of CBA must contain the contact details of all important roles.

9.9.3 Other staff's contact information may be published online only on the employee's consent.

10 SECURITY OF DOCUMENTS AND STORAGE

10.1 Archiving

10.1.1 Typical time for keeping archived materials is seven years.

10.1.2 In exceptional cases, which may result from the corresponding laws (Commercial Code, Law on Archives, rules for archival), or other considerations, the time is decided by head of sub-unit.

10.2 Keeping paper documents

10.2.1 Secret and confidential documents must be kept in fireproof safe.

10.2.2 Any other documents to be archived must be stored in archive room on shelves, in labeled folders and boxes.

10.2.3 The originals of technical documents must be kept in archive.

10.2.4 Other non-public documents must be kept in closed cabinets or drawers.

10.3 Keeping storage media

10.3.1 Media with secret contents must be kept in a safe.

10.3.2 Other significant (see 4.1.2.1-4.1.2.6) media should be labeled and maintained in archive.

10.4 Sanitization and disposal

10.4.1 Obsolete documents and data storage for disposal must be archived, and at the end of archival time physically destroyed.

10.4.2 Floppy disks must be sanitized by re-formatting before re-using them.

10.4.3 Defective media should be disposed when defects occur.

10.5 Transfer and admission procedures

10.5.1 Inter-authority transfer and adoption of documents and media should be documented.

10.5.2 The transfer by mail or other intermediary or channel of communication must be acknowledged by receipt of the guarantee.

10.5.3 See also Section 7.4 and 7.7.

11 BUSINESS CONTINUITY

11.1Backup

11.1.1 Data and software

11.1.1.1 Work data should be copied from workstation to server or through the server to the tape at least once a day.

11.1.1.2 From the server, documents, source code and user home directories must be copied to tape or CD at least once a week.

11.1.1.3 Static data should be copied to tape at least once a year.

11.1.2 Storage and testing of backups

11.1.2.1 Emergency copies are kept in opposite ends of the house in archive rooms.

11.1.2.2 Backup and restore functions must be tested on a regular basis.

11.1.3 Hardware

11.1.3.1 Hot spares are not justified due to lack of time-critical processes.

11.1.3.2 Maximal allowed outage of hardware is 12 hours during work time.

11.1.3.3 If necessary, replace faulty hardware component temporarily from another non-essential system.

11.1.4 Communication cables

11.1.4.1 Working cables are used as spare communication cables.

11.1.4.2 Fixed and mobile telephones are to be used as mutual spares.

11.1.5 Power

11.1.5.1 Acquisitions of additional power feeds or generators are not economically feasible.

11.1.5.2 Essential equipment and systems are backed up with batteries or UPS-es (see 8.3.4).

11.1.6 Premises

11.1.6.1 Backup office space is not available.

11.1.7 Technical and records

See 11.1.7.1 10.1-10.3.

11.1.7.2 Backup and single large copies of data too large for backup should be kept in a secure way.

11.2 Emergencies

11.2.1 The list of possible emergencies should be reviewed at least yearly.

11.2.2 If needed, establish contracts for possible fast of delivery of replacements.

11.2.3 Resources for the unexpected actions of at least acceptable residual risk must be taken into account in drawing up the budget of CBA.

12 CHANGE MANAGEMENT

12.1 Security monitoring

12.1.1 Operative monitoring

12.1.1.1 Security officers should review audit logs at least once a week.

12.1.1.2 On security incidents, possible security needs changes need to be identified.

12.1.1.3 On significant technical, organizational, legal or other internal or external changes, possible security need changes must be identified.

12.1.2 Random security checks

In subunits, the information security must be randomly checked at least once every two months.

12.1.3 Regular review of security

Must be performed at least once a year.

12.2 Security policy modification

12.2.1 The security policy is changed, if so required by the security monitoring results (see 12.1).

12.2.2 The security policy is amended, if the need arises from the appearance of a new version of baseline security directory.

12.2.3 Security Council makes the amendments in all cases, in no later than one week.

12.2.4 Security changes due to security policy changes are carried out within one month.