1 General

1.1 SUBJECT

This security policy involves the security of Comprehensive Benefits of America, LLC (CBA.) It consists of security objectives, guidelines for their achievement, and overall security management strategy and implementation of policies on crucial 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 SECURITY POLICY GOAL

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

1.4 **SECURITY OBJECTIVES**

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

1.4.2 Asset availability, integrity, and confidentiality must conform to an above-average level of security.

1.4.3 Compliance with the security legislation (including copyright, personal information, state laws and regulations, and workers' health and safety 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.

1.4.4 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.

1.5 SECURITY PRINCIPLES

1.5.1 Security platform provided by BridgePoint Technologies reduces the risk of viruses, Ransomware and loss of sensitive information. This service is referred to as "Zero Trust," and the specific platform is ThreatLocker.

1.5.2 Most cybersecurity protections are based on looking for, finding, and stopping threats. The problem is that cybercriminals are getting smarter and entering networks undetected, and bypassing legacy security systems.

End-users accidentally introduce threats by downloading various applications without validating them as authentic or trustworthy, clicking on links they shouldn't, and opening infected attachments in emails. That's why a new approach of blocking everything that is not trusted and only allowing those approved applications is a far safer and more comprehensive approach to ensuring malware does not end up on your networks.

1.5.3 ThreatLocker combines Application Whitelisting with Ringfencing and Storage Control in ways that make security simple. Zero Trust helps ensure that you and your device will not be exploited.

1.5.4 Controlling what software can run should be the first line of defense to better protect yourself against malicious software.

Ringfencing™ adds a second line of defense for applications that are permitted. First, by defining how applications can interact with each other, and secondly, by controlling what resources applications can access, such as networks, files, and registries. Ringfencing™ is an invaluable tool in the fight against file-less malware and software exploits.

1.5.5 Allowlisting has long been the gold standard in protecting businesses from known and unknown executables. Unlike antivirus, Allowlisting puts CBA in control over what software, scripts, executables, and libraries can run on our endpoints and servers. This approach stops not only malicious software but also stops other unpermitted applications from running. This approach greatly minimizes cyber threats by eliminating rogue applications from running on our network.

1.5.6 ThreatLocker® Storage Control is an advanced storage control solution that protects information. We have the tools to control the flow and access of data. We can choose what data can be accessed or copied and the applications, users, and computers that can access said data. By using ThreatLocker®, we control our file servers, USB drives, and your data. Most data protection programs on the market are butcher knife solutions to a problem that requires a scalpel. Blocking USB drives and encrypting data-storage servers can help secure our organization's private data. However, these tools don't consider that this Data needs to be utilized quickly.

1.5.7 CBA uses "Barracuda Email Security Service" – or "ESS." ESS is a cloud-based security service that protects both inbound and outbound emails against the latest spam, viruses, worms, phishing, and denial of service attacks. Any items deemed to be illicit will be quarantined in the ESS platform. Due to the sophistication of hackers, it is essential to reduce the risk by preventing emails with dangerous attachments or links to infected websites.

1.5.8 Assets usage permissions are granted to the workers based on work-related needs.

2 SECURITY ORGANIZATION AND INFRASTRUCTURE

2.1 Bob Fuhrman serves as our vCIO.

2.1.1 Our vCIO served as an IT Director in law firms for over 20 years, including a mid-sized national law firm with headquarters in Chicago.

He has extensive experience managing all aspects of IT in a professional services environment, including long-term strategic planning; vendor management; infrastructure design; backup, disaster recovery & business continuity; migration to cloud services; risk management; creating & managing a Help Desk, and designing ongoing training regimens.

3 PHYSICAL AND INFORMATION ASSETS

3.1 Critical Assets
This security policy mainly targets the security of assets listed in this section.

3.1.1 Infrastructure
The following items must meet a medium level of availability and integrity: premises technical Infrastructure, power distribution, and other general-purpose utility systems equipment and tools used for maintenance.

3.1.2 Data and documentation for CBA's activity, especially the following types of data, are essential security-wise:

3.1.2.1 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.

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

3.1.2.3 Self-produced data for which integrity and availability are essential: internal development's intermediate and final results, including self-made software.

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

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

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

3.1.2.7 Auxiliary data that needs availability and integrity: management data about Infrastructure, documentation for equipment and Infrastructure, and professional literature.

3.1.3 Hardware; the integrity and availability of the following Hardware are important: servers, workstations, notebooks, and network infrastructure equipment Peripherals are counted to belong with computers.

3.1.4 Communications systems, availability, and integrity of the following communications equipment are essential:
PBX (telephone exchange)
phone cabling and distribution devices telephones, including mobile phones, firewalls, routers, modems, wireless networking, and other data communications equipment
communication cabling

3.1.5 Software Availability, integrity, and legality of commercial and self-made software are essential.

3.1.6. Contains the software for the company's purposes. The source code of self-made software is confidential unless decided otherwise. Self-made software should be under copyright protection.

3.1.6.1 Purchased general-purpose software: Microsoft Windows 7 Professional, Microsoft Windows 10, and Windows 11 Professional

3.1.6.2 Obtain freeware only from trusted sources and agree with the vCIO and website developer.

4 **RISKS AND WEAKNESSES**

The following risks will be considered typical, and security measures are based on this selection.

4.1 Spontaneous risks

Fire
Thunderstorm
Water and fire extinguishing damages, including stormwater, emergency pipelines, etc.
Human error
Fluctuations in power quality and plain blackout
Hardware error
Interruption of external communications
Loss of Staff

4.2 Attacks

Theft
Viruses
Penetration into the internal network from the public network
Distributed Denial of Service (DDoS)
Sniffing of an internal computer network
Interception of oral communication
Workers' deliberate security breaching behavior, internal attacks

5 **SECURITY MEASURE POLICIES**

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

5.1 Access policy

5.1.1 Access to resources is role-based, according to job requirements.
5.1.2 IT user roles are defined by IT system features and from the structure of IT management.
5.1.3 IT ruleset must have at least three levels for access to Data: no access, read-only, and read-write.

5.2 Password management

5.2.1 Access passwords must be changed at least three times a year.
5.2.2 System, network, and other administrative passwords are stored, managed, and encrypted by LastPass. They are recognized as the best password management system for businesses, trusted by millions, and contracted by hundreds of businesses to keep their passwords secure.

5.3 Cryptography policy

5.3.1 For accessing internal network resources across the public network and confidential data transmission
across the public network, only secure connections must be used: VPN connections, SSL / HTTPS connections, and encrypted mail messages.
5.3.2 All confidential data on computers being carried outside the company perimeter (laptops, computers of home workers) must be encrypted, and all confidential data on hard disks. Encryption keys must be duplicated in a safe backup.
5.3.3 The minimum acceptable key length for symmetric encryption is 256 bits.
5.3.4 The minimum acceptable key length of asymmetric encryption is 1024 bits.

5.4 Logging and log reviewing policy

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

5.4.2 System and networking log checks must be performed randomly at least once a week after the respective incidents.
5.4.3 All logs must be stored for at least four weeks.

5.5 Removal policy

5.5.1 All unnecessary paper documents with confidential data are destroyed with a shredder.
5.5.2 Retired and discarded archive storage media must be destroyed physically.

5.6 Work environment

5.6.1 New software must be tested before use and confirmed to be suitable.
5.6.2 No accurate data must be used for testing and demos.

5.7 Legality policy

5.7.1 All assets must be acquired legally.
5.7.2 All uses of the assets must be legal.

6 **SECURITY OF COMMUNICATION**

6.1 Networking infrastructure

6.1.1 CBA network must meet the following two-level logical structure:
External network outside the firewall
Internal network inside the firewall.

7 **NETWORK MANAGEMENT**

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

7.2 Internal network management

7.2.1 The company has one shared internal network.

7.3 Servers

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

7.3.2 Besides the web serving, external web servers can only run FTP servers.

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

7.4 Email

7.4.1 Internal emails should not be sent outside the internal network (even in quoted form).
7.4.2 Mail sent to public networks must include the proper name of the sender.
7.4.3 Incoming and outgoing mail must be subjected to virus scanning.
7.4.4 Opening active contents (.EXE, VBS, etc.) in incoming emails are permitted only for security investigation purposes.
7.4.5 When possible, avoid sending documents in formats allowing macros.
7.4.6 Files attached to email must not contain parts of other files that do not show up with the viewer.
7.4.7 Our emails are protected by "Barracuda Email Security Service" – or "ESS."

ESS is a cloud-based security service that protects both inbound and outbound emails against the latest spam, viruses, worms, phishing, and denial of service attacks.

Many email threats today use social engineering tactics to target users and bypass email security gateways. We must stay ahead of cybercriminals to protect our business and your confidential data and documents.

Only Barracuda protects against all 13 email threat types.

Barracuda Email Protection provides the most comprehensive protection against all 13 email threat types, from spam and ransomware to socially engineered threats such as spear phishing, business email compromise, and account takeover.

Any items deemed to be illicit will be quarantined in the ESS platform.

Due to the sophistication of hackers, it is essential to reduce the risk by preventing emails with dangerous attachments or links to infected websites.

Each user receives email notifications once a day (or more frequently if so desired) listing messages which have been quarantined.

7.5 Phone calls

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

7.6 Fax

7.6.1 CBA's fax is used only by authorized personnel.
7.6.2 Fax modems of LAN workstations are connected to external networks.

7.7 Exchange of data using removable media

7.7.1 Materials transferred using a portable storage device or a CD must not contain any hidden data or other materials.
7.7.2 When receiving materials with a portable storage device, a 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 Confidential matters are avoided in public zones.

8 **GENERAL SECURITY**

8.1 Security of perimeter and zones

8.1.1 Doors

8.1.1.1 Corridor doors are self-closing and locked after hours.

8.1.1.2 The entrance to the building must be locked outside of working hours and only accessible by assigned key fobs.

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 requires. Internal rules govern admission at any other time.
8.1.2.2 The right to access 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 are kept in locked fireproof cabinets or off-premises.

8.1.4 Visitors

8.1.4.1 Visitors are allowed in the building of CBA only when checked in by the receptionist.
8.1.4.2 Meetings, seminars, and other events where other parties are involved only take place in the 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 do not appear in building guides.

8.2.2 Fire alarm system

8.2.2.1 Fire alarm sensors are installed according to the 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 complies with fire regulations.
8.2.3.2 The fire extinguishers in rooms with computers or electricity distribution are powder-based.
8.2.3.3 Staff are instructed to use fire extinguishers.

8.2.4 Environmental measures

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

8.2.5 Security of premises

8.2.5.1 When leaving the workplace, the workers must lock the door.

8.2.6 Workplace security

8.2.6.1 All workplaces comply with the principle of an empty table, i.e., when leaving the room after work, remove all the documents and media from the table and other visible locations, and lock the computer screen.
8.2.6.2 Important documents, media, and small but valued physical assets are kept in a locked cabinet or drawer.

8.2.7 Maintenance and repair work

8.2.7.1 External maintenance and repair personnel is allowed to the premises only when accompanied by an attendant.
8.2.7.2 At any given time, only the minimum required several rooms must be opened for maintenance and repair.
8.2.7.3 Keys or other access devices are not 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 the CBA office only with the permission of the 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 unique cabinets.

8.3.4 Interruptions in technical services

8.3.4.1 Server backup power must be provided using UPS for at least 5 minutes.
8.3.4.2 Alarm system must have an emergency power supply with batteries for at least 48 hours.

8.4 Communication with the authorities in case of the security incident

8.4.1, The employee who discovered the danger will contact the police or 911.
8.4.2 Communication specialist will deal with network service providers
8.4.3 On electricity issues, the security officer interacts with the relevant authorities.

9 **PERSONNEL SECURITY**

9.1 Staff Selection

9.1.1 Candidates for vacant jobs are selected based on job requirements.

9.1.2 Each candidate's background is 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 in each case.
9.2.3 Head of the department is responsible for instructing 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 following events must be announced:
security incidents
security environment changes

recruitment and dismissal
changes and additions to the internal network security system

9.4 Procedures for dismissal

9.4.1 By the end of the last working day, the dismissed worker must return all assets to the CBA Department head responsible for the take-back.

9.4.2 By the end of the last working day, all means of access (keys) and credentials must be removed (change the passwords, remove from access control lists). The Department head is responsible for the take-back.

9.4.3 If necessary, the measures in 9.4.1 and 9.4.2 are taken immediately after the dismissal decision.

9.5 Penalties

9.5.1 In case of breach of security requirements, the offender will be prosecuted with penalties ranging from a public reprimand to dismissal.
9.5.2 CBA directorate must make the offender compensate for caused physical damage.

9.5 Telework

9.5.1 Teleworking is entitled case by case.
9.5.2 Teleworking may be conducted only through secure communications and in compliance with other appropriate security requirements.

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 the head of the sub-unit.

10.2 Keeping paper documents

10.2.1 Secret and confidential documents must be kept in a fireproof safe.
10.2.2 Any other documents to be archived must be stored in the archive room on shelves, in labeled folders and boxes.
10.2.3 The originals of technical documents must be kept in the 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 media is labeled and maintained in the archive.

10.4 Sanitization and Disposal

10.4.1 Obsolete documents and data storage for disposal must be archived and physically destroyed at the end of archival time.
10.4.2 Floppy disks are sanitized by re-formatting before re-using them.
10.4.3 Defective media are disposed of when defects occur.

10.5 Transfer and admission procedures

10.5.1 Inter-authority transfer and adoption of documents and media are documented.
10.5.2 The transfer by mail or other intermediary or channel of communication must be acknowledged by receipt of the guarantee.

11 **BUSINESS CONTINUITY**

11.1 Backup

11.1.1 Data and software

11.1.1.1 Work data is copied from the workstation to the 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 are copied to an external hard drive at least once a week.

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

12 **CHANGE MANAGEMENT**

12.1 Security Monitoring

12.1.1 Operative monitoring

12.1.1.1 Security officers review audit logs at least once weekly.

12.1.1.2 Possible security need changes are identified as significant technical, organizational, legal, or other internal or external changes.

12.1.2 Random security checks

12.1.2.1 Information security must be randomly checked in subunits at least once every two months.

12.1.3 Regular review of security is performed at least once a year.

12.2 Security policy modification

12.2.1 The security policy is changed if 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 the baseline security directory.

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

Updated 12/18/22