How Do We Securely Manage Your Data and Privacy

Since the beginning of VBP, we made a commitment to Information Security being an integral part of our business. From day one, we have put in place proper systems to ensure that both our company's and our clients' information are protected and secured.

Over the past almost 6 years, we have stood by this commitment and have gone through numerous due diligence processes with various stakeholders, Information Security audits as well as continuous development and expansion in our systems.

In 2018, we commenced the process of preparing the business for ISO 27001 certification. ISO 27001 is a globally recognised international standard for information security management.

In 2019, VBP successfully went through the ISO certification audit process and is now ISO 27001 certified.

We, in VBP, will strive to ensure that we have up-to-date and comprehensive systems in place to continue our commitment to Information Security – securing not only ours, but your business' and your clients' confidential data and assets.

David Deegan
Director of Operations
October 2019

ISO 27001
BUREAU VERITAS
Certification
BUREAU VERITAS
1828
UKAS
MANAGEMENT
SYSTEMS
0008

ISMS FAQs

VBP Management is committed to the control and security of all information.
VBP invests in education, training and IT infrastructure provided to its personnel to improve efficiency and ease of use, with the emphasis on the security of information.

The **INFORMATION SECURITY MANAGEMENT SYSTEM** is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

Below are the FAQs about our information security management system:

Governance

What governance arrangements does the entity have in place to implement and maintain its information security plans and measures?
The information security of VBP is designed to comply with ISO/IEC 27001:2013. This requires the organization to be compliant with all the legal and other requirements applicable to the business. We emphasize the compliance of any regulatory requirement on data privacy and information security.

Standards

What standards, if any, does VBP comply with?
VBP's information security is aligned to comply with ISO/IEC 27001:2013.
The ISMS risk assessment is structured to comply with ISO 31000:2018.
The internal audit is designed to go along with ISO 19011:2018.

How does the entity determine which standards to adopt?
The top management chose to pursue the ISO/IEC27001:2013 certification due to the nature of work and business the organization has. VBP commits to protect all data and information.

Access Control

What access controls are in place in VBP?
Access to an organization's data and information is critical and can lead to an illicit admission and leakage of confidential information.

Good access control processes determine who will be granted access to particular resources and under controlled conditions.
VBP is managing the admittance of any personnel to system and network resources by granting approval and restraining unauthorized access.

How is VBP managing the Access Rights of the employees?
Access rights shall determine the level of access needed and type of restrictions to be given to VBP personnel depending on their roles and responsibilities, client requirements and specific tasks.

How do you control access to personal gadgets?
VBP is not allowing all personally owned gadgets or mobile devices (phone, tablet, iPad USB, SD card, external hard drive and other gadgets with the same function) at the workstations to protect all client information and all workings without proper approval.

How is VBP managing employee's access to accounts?
All employees are provided with unique credentials to be used to access the work computer.

Employees are required to lock the computers when they leave their desks, even for a short time to prevent unauthorized access. This is emphasized during the ISMS induction. To add a layer of security, the computers are programmed to be automatically locked if left inactive or unattended for a certain period.

User accounts are locked out after a specified number of failed logins occur. Personnel is required to contact IT to unlock the user account.

Encryption

What are the cryptographic controls of VBP?
Encryption is a type of security that converts data, programs, and other information into unreadable code.

As Virtual Business Partners understands and promotes the confidentiality of information shared from or to the client, VBP requires minimum requirement encryption.

How do you manage passwords in VBP?
VBP uses a password manager, provides a personal dashboard for the deployment and management of passwords. All sensitive information stored in the password manager and is encrypted using standard encryption to ensure complete security and strong password generation for web and software applications.

For all accounts, a password shall need to meet the IT security requirements stated under VBP's password management.

All VBP Personnel shall need to redo their password every 90 days.

How do you protect Files, Workstation, Database, and Server?
VBP uses a security feature to encrypt confidential files, workstations, database, and servers with its default encryption algorithm for security. This ensures the integrity of the system that assists in securing personnel's data on desktop and laptop computers.

Do you protect your Network System?
VBP uses a firewall, a network security system designed to prevent unauthorized access to/from a private network connected to the internet. All VBP data at rest is encrypted using the AES encryption standard.

How do you secure Emails and Messages?
VBP uses an email application in which emails and messages are encrypted with the use of encryption protocols and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES).

How do you secure Websites and Software Applications?
VBP ensures that the internal websites used are secured with HyperText Transfer Protocol Secure (HTTPS).

HTTPS is a standard technology to keep an internet connection secure which safeguards any sensitive data that is being sent between two systems, preventing an unauthorized person from reading and modifying any information transferred. It uses encryption to scramble data in transit, preventing hackers from reading it as it is sent over the connection.

Are there procedures governing the printing of documents containing personal information?
The data transfer is encrypted on the Terminal Server (TS) then sent to the printer and then decrypted in the printer.

IT is responsible for monitoring printer updates and network security.

Staff members working directly with clients do not have access to printers, only a very limited number of operations staff have access to printers.

Any VBP personal requiring access to the Network printer must be approved and IT is required to configure the authorized personnel's computers.

Backup

Do you have a documented procedure for backing up data?
VBP has an establish back up and restoration procedure. This is to minimize the risks associated with data loss by defining a sound backup regime for all centralized Virtual Business Partners data services. This will ensure the safety and security of IT system resources and supporting assets.

Are backups set up to run frequently?
There are different backup methods used for different data depending on the source of data and information's importance. An established schedule of backup is done by the IT outlined in the procedure.

Does the entity review its backups to check that personal information that is no longer needed is deleted? How far back is data recoverable?
We test backups to ensure they are recoverable, not to review all information contained in the backup, they are recoverable for the past 7 days.

Are backups stored remotely to protect from natural disasters?
VBP's backup and restoration are done by the commissioned IT, which is in a different location from VBP's office.

Data Breaches

Is there a data breach response plan and does it flow logically from any broader information security plan?
VBP has an established Incident Response and Investigation Procedure for incidents, which threatens the preservation of confidentiality, integrity, and availability of resources and information. Information security incidents can cover a multitude of situations, but generally, it involves an adverse event that results or has the potential to result in the compromise, misuse or loss of VBP owned information or assets.

Does the plan include a strategy to assess and contain breaches?
To determine the level of investigation required, VBP classifies the incidents to enable the appropriate prioritization of incident response and level of investigation. Incidents are rated following a level of risk, which is based on agreed criteria for assessing the consequence, likelihood, and impact of risk.

Are staff educated about the plan and how to respond to data breaches?
All employees have undergone ISMS Induction. This gives emphasis on educating staff on how to respond to information security breaches.

Does the plan enable staff to identify data breaches and require that breaches be reported?
All information security incidents are immediately reported after the personnel is made aware of a potential or actual incident.

Once an incident has been positively identified, I.T. shall work with appropriate personnel to isolate the affected equipment in order to prevent secondary threats, attacks on other internal systems, and potential legal liability, including blocking network access.
Incidents may include but not limited to:

- Suspected or actual disclosure, loss of information or inappropriate exposure of information to an unauthorized recipient
- Abnormal systematic attempt to compromise information
- Suspected or actual weakness in the safety net protecting information.

The compromised system or user account that is actively causing widespread problems or affecting none VBP network or computer shall be blocked immediately.
Other immediate actions may include removal from service or forensic analysis if appropriate. Our IT support group may recommend additional containment measures in addition to those outlined in this procedure.

Does the plan outline clearly when affected individuals should be notified of breaches?
While isolated incidents may be resolved with minimal involvement outside IT Management, some incidents may require escalation to notify appropriate entities, to obtain investigative information or assistance, and to ensure an appropriate public response by the company.
Four escalation levels are outlined as follows:

- Initial
- Department Level
- Company Level
- External.

Does the plan include a strategy to identify and address any weaknesses in data handling/data security that contributed to the breach?
All recommendations and corrective actions identified shall be entered into the Corrective Actions Register, along with a responsible person nominated to complete the required action/s and a completion date.

The investigation is considered closed when all reports are completed, and evidence is documented and filed. The Management team will conduct the final review of the report and actions taken to form the recommendation from the investigation. This allows assessment of the investigation and identifies any potential improvements to investigation practices.

Physical Security

Is the area of operations secured?
All entry points around VBP's facility were risk assessed including ceiling, walls and emergency exits to ensure a good degree of protection is in place and with no weak points.

External doors are secured with a level of additional protection appropriate to the required security level with due consideration of applicable fire safety regulations.

The secure area is designed in a way that sensitive information cannot be viewed from public areas. Screens that may contain sensitive information are positioned away from where unauthorized personnel may view them.

Reception
VBP has a defined reception area through which all access is controlled. The reception area is adequately manned when the VBP site is open and only authorized personnel will be admitted.

Entry Controls for Visitors
All visitors shall sign in at reception and record details of their identity and time of entry and departure. Visitor access to the secured area is requested in advance and should be supervised by authorized personnel within VBP.

Physical Barrier
CCTV cameras are installed within strategic locations to ensure personnel's safety and security by preventing crime, preventing personnel misconduct and ensuring compliance with company policies and procedures.

Biometric scanners are installed to prevent access without the correct level of authorization. Tailgating is strictly prohibited.

All personnel is required to wear a visible and current ID badge for identification.

How do you have a public area, delivery area, and loading area?
A separate delivery or holding area is provided and deliveries are inspected prior to them being accepted in the secured area. The area is designed such that deliveries and outgoing items are not stored in the same place.

Delivery personnel is accompanied by an authorized employee should there be a need for them to get in.

Regular monitoring and review

Does the entity regularly monitor and review the operation and effectiveness of its information security measures?
VBP has established a range of metrics to measure and evaluate how well the ISMS is performing. The specific plans to achieve each objective and Key performance indicator are established in the Objectives and Targets Register.

Change management

How are changes being handled by the organization?
Changes in the organization shall be identified based on the needs of the business. Whenever the need for a change, a change owner shall be appointed. Those affected by the change shall be identified, recorded and notified of the proposed change by the change owner. Any changes within the organization shall undergo a review and approval process.

Do you conduct a risk assessment prior to conducting a change within the organization?
Yes, the change owner shall ensure that a risk assessment is conducted considering the nature, timescale, and scope of the change.

The risk assessment shall consider the impact of the change before, during and after the change and include consideration of the potential for:
- Effects/Stop operation
- Damage to equipment
- Loss of data information
- Adverse effects to the process being changed, any upstream and downstream processes and any supporting processes.

Consideration is given to the technical merits of undertaking the change.
Where appropriate, the change owner shall ensure the proposed change is reviewed and approved by IT from a technical perspective.

Education and Training

Is education/training given to provide staff with an awareness of information security? How often is this education given? Is the training targeted to specific audiences?
VBP provides ongoing education about information security to all employees.
New employees are required to finish information security training upon starting. They need to complete and pass our online learning management systems courses on privacy and information security. During new hire induction, their immediate head walks them through and explains the company policies relating to privacy and information security. Tenured employees are enrolled in an online course at least annually. In addition, frequent information security reminders are cascaded via email monthly.

Risks

How do you track and manage your information security risks? Do you use a specific framework?
The ISMS Risk assessment provides the foundation of the VBP Information Security Management System. This outlines the Information assets, the source of potential risks, vulnerabilities and information security scenarios and impacts to the organization and the lists of controls required to mitigate the potential risks that VBP is exposed to.

The ISMS risk assessment is structured to comply with ISO 27001:2013 and ISO 31000:2018.
VBP management and key personnel have been involved with its developed.

VBP's risk assessment is evaluated annually.

How do you identify and monitor potential security incidents?
Our managed services agreement with our IT provider includes 24/7 monitoring of all our endpoints. This proactively monitors all of the potential risks, threats, vulnerabilities and general issues.

We are notified when warnings are triggered enabling us to mitigate these issues quickly and effectively before they become problems.

When an alert gets triggered this gets sent to our IT providers help desk ticketing system and automatically turned in to a ticket and assigned to a tech support with a priority level set.
The help desk is then responsible for actively monitoring and resolving the incident.

What is currently being done to protect your IT environment against known and unknown vulnerabilities? What tools are being used?
Our proactive and regular weekly maintenance program includes patching of all systems and remediating known vulnerabilities and mitigate threats.

The vulnerability of the VBP's ISMS is being managed by ensuring all relevant information about VBP's information assets, like software manufacturer, software version, where the software is installed, and who is responsible for each piece of software is maintained.

Do you have any detailed incident management procedure including response and recovery?
VBP has an established incident response and investigation procedure. This provides VBP a framework for IT incident handling process, which threatens the preservation of confidentiality, integrity, and availability of resources and information.
VBP has put in place a number of technical measures to safeguard the data and information it owns. This includes technical security, physical building and office security to procedural requirements for safe handling and storage of information.
Business Continuity Plan has been established to manage recovery of critical business functions in managing and supporting business recovery in the event of business disruption.