



VBP ENABLING LICENSEES TO MEET ASIC OBLIGATIONS ON OFFSHORE OUTSOURCING



Our Information Security
Management System
is certified in accordance with
ISO/IEC 27001 standards.

VBP's Approach

		VBP
Q1	Governance & Risk Management Frameworks	✓
Q2	Due Diligence in OSP Selection	✓
Q3	Ongoing Performance Monitoring	✓
Q4	Access Log Monitoring & Alerts	✓
Q5	Independent Cybersecurity Assessments	✓
Q6	Data Privacy & Legal Compliance	✓
Q7	Support for Licensee Oversight	✓
Q8	RG10 - APS licensing: Meeting the general obligations	✓

VBP ENABLING LICENSEES TO MEET ASIC OBLIGATIONS ON OFFSHORE OUTSOURCING

Following ASIC's report into offshore outsourcing practices, VBP remains committed to supporting Australian Financial Services (AFS) licensees and their authorised representatives in meeting their regulatory obligations.

Below is a summary of how VBP aligns with ASIC's expectations:

1. Governance & Risk Management Frameworks

VBP maintains a governance and risk management framework that meets the standards set out in Section 912A(1)(h) of the Corporations Act 2001, ensuring compliance with ASIC's requirement for adequate risk management systems. Our internal controls, compliance programs, and ISMS risk assessment, aligned with ISO 27001:2022 and ISO 31000:2018, collectively support the identification, mitigation, and monitoring of risks across the organisation. This framework is reviewed annually and actively supported by senior management to ensure ongoing regulatory alignment and operational resilience.

2. Due Diligence in OSP Selection

VBP provides onboarding documentation to support clients and licensees in meeting their due diligence obligations. Our onboarding materials include detailed insights into our operational structure, governance frameworks, service delivery models, and compliance alignment with AFSL requirements. These resources are designed to streamline the evaluation process and enable licensees to make informed decisions with confidence.

We maintain full transparency across our operational capabilities, data handling procedures, and security protocols. This includes documented workflows, business continuity plans, and robust information security measures that demonstrate our commitment to regulatory compliance and data protection.

Importantly, we actively welcome and regularly receive due diligence requests from clients and licensees and have successfully completed due diligence processes with listed companies. We view

this as a critical part of maintaining trust and accountability in our partnerships. Our team is responsive and collaborative in providing the necessary documentation, clarifications, and access to support thorough assessments.

By offering this level of visibility and engagement, VBP empowers licensees to uphold their regulatory responsibilities while benefiting from a reliable and compliant outsourcing partner.

3. Ongoing Performance Monitoring

VBP maintains a structured performance monitoring framework aligned with ASIC's obligations under RG 104 and RG 166. This includes audit trails, service level reports, KPI dashboards, and monthly progress reviews to ensure transparency, accountability, and continuous improvement. Our 88.1% favourable CSAT rating reflects consistent service quality, with tailored development plans deployed to address performance gaps.

We engage proactively with clients and licensees to identify improvement opportunities, supported by clear escalation pathways, ongoing training, and onboarding process. These mechanisms ensure compliance with contractual and regulatory standards.

4. Access Log Monitoring & Alerts

VBP maintains a dedicated cybersecurity team responsible for overseeing access log monitoring and real-time alerting across all systems. This team ensures that all user activities are captured through detailed access logs, enabling traceability, audit readiness, and forensic analysis when needed.

Real-time alerts are configured to detect unauthorized access and anomalous behaviour, allowing immediate investigation and response. These controls support proactive risk mitigation, continuous monitoring, and compliance with ASIC's principles of cyber resilience and operational integrity.

5. Independent Cybersecurity Assessments

VBP undergoes regular independent information security assessments conducted by qualified external auditors as part of our certification maintenance, ensuring objectivity and rigor in evaluating our information security posture. These assessments are aligned with ASIC's expectations for financial services firms,

including the need for independent assurance over cyber risk management practices. Results are shared with relevant stakeholders, including executive leadership to foster accountability and continuous improvement.

Our cybersecurity framework is built on internationally recognised standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework, and incorporates controls recommended by the Australian Cyber Security Centre (ACSC). This ensures resilience against evolving threats and supports compliance with regulatory obligations under the Corporations Act and ASIC's RG 255 guidance on cyber resilience.

VBP also maintains a governance structure, with cybersecurity oversight embedded at the board and executive levels, and integrates threat intelligence, incident response planning, and third-party risk management into its broader risk and compliance program.

6. Data Privacy & Legal Compliance

VBP adheres to the Australian Privacy Principles (APPs) and ensures that its offshore operations comply with all relevant data protection laws. As part of our commitment to privacy and regulatory compliance, VBP is registered with the National Privacy Commission (NPC) in the Philippines and has appointed a dedicated Data Privacy Officer to oversee data governance and protection practices.

We provide transparency around jurisdictional risks and implement contractual safeguards to mitigate exposure to foreign legal conflicts, ensuring our clients' data remains secure and compliant across borders.

7. Support for Licensee Oversight

VBP empowers licensees to maintain oversight and control over outsourced functions through transparent reporting, structured escalation protocols, and collaborative governance frameworks.

We support the identification and management of material risks and provide practical solutions to assess the ongoing suitability of outsourced services. Our approach aligns with ASIC's expectations for licensee oversight, ensuring compliance and accountability across all service engagements.

8. RG104 - AFS licensing: Meeting the general obligations

The table below summarises how VBP's ISMS practice aligns to and supports obligations under Regulatory Guide 104, which outlines the general obligations that Australian Financial Services (AFS) licensees must comply with under the Corporations Act.

RG104 Obligation	VBP ISMS Practice
Efficient, honest, and fair service delivery	Mandatory onboarding, client satisfaction survey, refresher training, progress reviews, SOPs and policies for WFH and other ISMS related, encryption, access controls, and SLAs
Adequate Risk Management Systems	Annual ISMS risk assessment aligned with ISO 31000:2018; Risk register; Incident, Response and Investigation Procedure
Technological Resources	Endpoint protection, active monitoring, encryption, password management, backup procedures, patching, and vulnerability management
Incident response and breach management	Incident Response & Investigation Procedure; escalation levels; corrective actions register
Team Member training and awareness	Team Member onboarding, annual refresher, quarterly advisories, phishing awareness and simulation
Third-party oversight	Visitor NDA, delivery inspections, access control, software whitelist and approval process, supplier vetting and evaluation
Access control and authentication	Role-based access, MFA, device restrictions, USB port lockdown, credential uniqueness, SSO, geo blocking, user registration and de-registration procedure
Data classification and handling	Public/Internal/Confidential classification; default to Confidential; auto-deletion policy

RG104 Obligation	VBP ISMS Practice
Physical and environmental security	Risk assessment for all entry points, CCTV, RFID, visitor logs, reception control, workstation layouts
Monitoring and review	Internal audits, external audits, KPIs in Objectives and Targets Register, supplier and contractor evaluation, client satisfaction survey, team member satisfaction survey, client onboarding survey, refresher training, active monitoring, monitoring of IT-related incidents
Change management	Risk-based change approval, stakeholder consultation, technical review
Business continuity	Business Continuity Plan; Backup and Restoration Procedures, Business Impact Assessment, BCP Post-Mortem
Hybrid work security	WFH Security Matrix, encryption, web filtering, SOPs, endpoint protection, Offsite Work Policy and other ISMS related policies

INFORMATION SECURITY MANAGEMENT SYSTEM FAQs

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

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

Below, are the frequently asked questions (FAQs) regarding 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 27001:2022. This requires the organisation 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 compliant with ISO/IEC 27001:2022. The ISMS risk assessment is structured to comply with ISO 31000:2018. The internal audit is designed to ensure compliance with ISO 19011:2018.

How does the entity determine which standards to adopt?

The top management chose to pursue the ISO/IEC 27001:2022 certification due to the nature of work and business the organisation has. VBP commits to protect all data and information.

Access Control

What access controls are in place in VBP?

Access to an organisation'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.

We are managing the admittance of any Team Member to system and network resources by granting approval and restraining unauthorised access.

How is VBP managing the Access Rights of the Team Members?

Access rights shall determine the level of access needed and the type of restrictions to be given to VBP Team Member depending on their roles and responsibilities, client requirements and specific tasks.

How do you control access to personal devices in the workplace (office)?

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. For unique circumstances, proper approval must be secured prior to using non-VBP devices for work.

Access to mobile devices is limited to the use of multi-factor authenticators exclusively for work purposes. This is stated in our company policy.

How is VBP managing Team Member's access to accounts?

All team members are assigned with unique credentials to facilitate secure access to their work computers.

Accounts are not accessible on non-VBP devices. Only individuals who have received approval, according to their specific roles, may access their accounts via personal devices.

To maintain the security of our work environment, team members are required to lock their computers when leaving their desks, regardless of the duration of their absence. This protocol is emphasized during the ISMS Team Member onboarding process. Furthermore, to enhance security measures, computers are configured to automatically lock after a designated period of inactivity or when left unattended. In the event of multiple unsuccessful login attempts, user accounts will be locked for security purposes. Team members will need to reach out to VBP IT to have their user accounts unlocked.

Encryption

What are the cryptographic controls of VBP?

Encryption is a type of security that converts data, programs, and other information into unreadable code.

We understand and promote the confidentiality of information shared from or to the client. As best practice, we uphold minimum encryption requirements as stated in the cryptographic procedure.

How do you manage passwords in VBP?

We use a designated password manager to provide a personal dashboard for deployment and management of passwords. All sensitive information is stored within the password manager and is encrypted using standard encryption. This ensures complete security and strong password generation for web and software applications.

For all accounts, a password shall be needed to meet the IT security requirements stated in our password management guidelines.

All VBP team members must reset their passwords every 90 days. Automated password rules and policies have been deployed to all VBP equipment to enforce password expiration, prompting team members to comply.

How do you protect Files, Workstations, Databases, and Server?

We use a security feature to encrypt confidential files, workstations, databases, and servers with its default encryption algorithm. This ensures the integrity of the system and assists in securing team member's data on desktop and laptop computers.

Do you protect your Network System?

We use a firewall, a network security system designed to prevent unauthorised 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?

We use an email application that encrypts emails and messages with encryption protocols and technologies including Transport Layer Security/ Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES).

The messaging tools are encrypted using cryptographic keys only available to the team members and uses HTTPS for network environments. This ensures no third party can access these keys.

How do you secure Websites and Software Applications?

We ensure that the internal websites we use are secured with HyperText Transfer Protocol Secure (HTTPS).

HTTPS is a standard technology to keep an internet connection secure and safeguards any sensitive data that is being sent between two systems, preventing an unauthorised 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.

VBP ensures that all installed software applications meet the minimum encryption standards. The IT Infra Team identifies which software needs updates, while the IT Support Team is responsible for updating these software packages to maintain security.

Are there procedures governing the printing of documents containing personal information?

The data transfer is encrypted on the Terminal Server (TS) then sent and decrypted in the printer.

Our VBP IT Team is responsible for monitoring printer updates and network security.

Team members working directly with clients do not have access to printers, only a very limited number of support team members have access to printers.

Any VBP Team Member requiring access to the Network printer shall be approved first. IT is required to configure the Team Member's equipment in accordance with the approval given. Access to network printer is monitored and audited on regular period.

Software

Do you have measures in place to control software installations on Team Members' assets?

Team Members do not have the capability to install any applications in VBP Assets due to the technical control put in place to restrict any installations. Only IT team are allowed to install approved applications according to the Whitelist register.

For applications not on the whitelist, we follow a Software and Hardware Request Procedure. This procedure involves evaluating the requested software and obtaining a series of approvals before installing it on a team member's asset.

Backup

Do you have a documented procedure for backing up data?

We have an established backup and restoration procedure. This is to minimise the risks associated with data loss by defining a sound backup regime for all centralised VBP data services. This will ensure the safety and security of IT system resources and supporting assets.

Are backups set up to run frequently?

There is different backup methods used for different data depending on the source of data and the 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 tested backups to ensure they are recoverable for the past 7 days. VBP does not store personal information that is no longer needed. This is part of our policy.

Are backups stored remotely to protect from natural disasters?

All Data for VBP is backed up via Cloud and using multiple platforms.

Data Breaches

Is there a data breach response plan and does it flow logically from any broader information security plan?

We have an established Incident Response and Investigation Procedure for incidents that threatens the preservation of confidentiality, integrity, and availability of resources and information in compliant with the requirements of Notifiable Data Breach Privacy Act 1988 and RA 10173 Data Privacy Act of 2012. Information security incidents can cover a multitude of situations, but generally, they involve 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, we classify the incidents to enable the appropriate prioritisation 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 Team Members educated about the plan and how to respond to data breaches?

All Team Members have undergone ISMS Team Member Onboarding that includes a topic focusing on educating team members on responding to information security breaches.

The RCRA Team along with the coordination of L&D Team, requires all tenured team members (six months and above) to complete the annual ISMS Refresher Course that will serve as their continuous awareness to the VBP's ISMS Program and the best practices in the industry. This will ensure that all team members are aware of how to respond to any possible data breaches that might occur in the organization.

In addition to the annual ISMS refresher course, the RCRA Team releases quarterly ISMS advisory to give constant reminders to Team Members of the company's ISMS policies and best practices in safeguarding the information assets of VBP.

Does the plan enable team members to identify data breaches and require that breaches be reported?

All information security incidents are immediately reported after the team member is made aware of a potential or actual incident, and as per required by law.

Once an incident has been positively identified, our Technology and RCRA teams shall work with affected team members to isolate the infected equipment to contain and prevent secondary threats, attacks on VBP systems.

Incidents may include but are not limited to:

- Suspected or actual disclosure, loss of information or inappropriate exposure of information to an unauthorised 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 the VBP network or computer shall be blocked immediately. Other immediate actions may include isolation of the equipment, removal from service or forensic analysis, if necessary. 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, obtain investigative information or assistance, and 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?

Every incident is investigated to identify the root cause. Then, risk assessment is conducted using the details derived from the investigation. Immediate and corrective action is established based on the identified root cause. All recommendations and corrective actions identified shall be entered into the Corrective Actions Register, along with an identified responsible person to ensure completion and implementation of the corrective action plan.

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.

Information and Asset handling

How do you classify information in VBP?

Information and assets are classified regarding its value, legal requirements, sensitivity and criticality to VBP. If the information is subject to classification, it shall be classified upon creation by the document owner according to the following guidelines below and shall be re-classified when there is any significant change in content.

- **Public** - The information is specifically for public access. There is no adverse impact resulting from publication. (i.e website, article, research that has been released).
- **Internal** - The information is not for public access but rather for internal use within the organisation. Accidental or unauthorised access to the information could potentially lead to significant damage to the business reputation.

- **Confidential** - The information is not for public access and restricted to a defined recipient. Accidental or unauthorised access to the information may result in serious reputational damage, financial and legal impact.

All client data and information are classified as “Confidential”. If the classification is uncertain, it is advised to use the default category as “Confidential”.

How do you store information in a way that would not allow anyone other than the client and assigned team member to gain access?

The general principle is that we do not store data. Instead, Team Members securely access and work on our client's data where it is stored. Any information that might be held locally is typically Work in Progress (WIP) and only temporarily within a managed environment and/ or endpoint. For example, XPLAN requires local exportation to the desktop version of Word for Statement of Advice generation. Modern cloud suites, including Microsoft's cloud version of Word, do not support the legacy formatting coding or programing utilized by third parties eg. VBA and others.

VBP implements an auto-deletion policy on its equipment to ensure that no files are stored locally. This policy is executed on a regular basis to maintain data security and compliance.

Physical Security

Is the area of operations secured?

All entry points around VBP's facilities were risk assessed including ceilings, 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 unauthorised team members 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 authorised team members 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 including the signing of the Visitor's Non-Disclosure Agreement. Visitor access to the secured area is requested in advance, and such visitors should be supervised by authorised team members within VBP.

Physical Barrier

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

Radio Frequency Identification (RFID) devices are installed to prevent access without the correct level of authorisation. Tailgating is strictly prohibited.

All Team Members are 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 are accompanied by an authorised Team Member should there be a need for them to get in.

Regular monitoring and review

Does VBP 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 indicators are established in the Objectives and Targets Register.

We also conduct internal audits to evaluate the effectiveness of our ISMS. Apart from that, we also undergo an annual external audit to maintain our certification to ISO/IEC 27001.

Change management

How are the changes being handled by the organisation?

Changes in the organisation shall be identified based on the needs of the business. Whenever a need for change is identified, 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 organisation shall undergo a review and approval process.

Do you conduct a risk assessment prior to conducting a change within the organisation?

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:

- Threat Operation
- Damage to equipment
- Loss of data information
- Adverse effects to the process being changed, any upstream and downstream processes and any supporting processes
- Business Strategy
- Financial Impact
- Process
- People and Culture

Consideration needs to be given to the technical merits of undertaking the change. Where appropriate, the change owner shall ensure the proposed change is reviewed and approved by the Subject Matter Expert from a technical perspective. Relevant VBP Stakeholders shall be consulted to assess and scope out possible impact areas. The controls and technical review outcomes are to be recorded.

Screening and Training

Do you perform the appropriate background and verifications checks prior to hiring a potential Team Member?

Pre-employment screening is undertaken by VBP and includes reference check, character check, NBI clearance requirement (which is equivalent to a police certificate in the AUS) or working with children check if required, pre-employment medical and fitness for work evaluation as required. Copies of relevant certificates confirming qualifications is obtained from candidates prior to an offer of employment.

Is education/training given to provide team members 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 Team Members. New Team Members 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 the new hire ISMS Team Member Onboarding, their immediate head walks them through and explains the company policies relating to privacy and information security.

Tenured Team Members 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 organisation 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 27001:2022 and ISO 31000:2018. VBP management and key team members have been involved with its development.

VBP's risk assessment is reviewed and evaluated annually.

How do you identify and monitor potential security incidents?

Our IT Team is tasked with the comprehensive management of all endpoints. The deployment of our automated policy enables the team to proactively monitor and mitigate potential risks, threats, vulnerabilities, and general issues, ensuring robust security and optimal performance.

All relevant stakeholders are notified when warnings are triggered, allowing us to address these issues quickly and effectively before they escalate.

When an alert is triggered, it is sent to our IT ticketing system, automatically converted into a ticket, and assigned to the IT Infra team with a designated priority level. They are then responsible for actively monitoring and resolving the incident

What is currently being done to protect your IT environment against known and unknown vulnerabilities?

We have a proactive maintenance program that includes daily for patching all systems, remediating known vulnerabilities and mitigating threats.

The vulnerability of VBP's ISMS is being managed by ensuring the maintenance of 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.

Do you have any detailed incident management procedures including response and recovery?

VBP has an established incident response and investigation procedure. This provides VBP with a framework for the 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.

A Business Continuity Plan has been established to manage the recovery of critical business functions in managing and supporting business recovery in the event of business disruption.

Hybrid Work Arrangement

Hybrid work has transformed the way many people work. In line with that, VBP has developed and used a diverse network setup and information security protocols to accommodate flexible working arrangements to provide Team Members the ability to work remotely.

Below are a few of the many setups we have integrated to ensure that VBP's Information Security Management System is still being upheld and replicated with Team Members under the Hybrid Work Arrangement.

How do you ensure team members remain alert and attentive to Information Security as there may be more spam email (e.g. phishing attempts) at this time?

As part of our Information Security Management System, we provide ongoing security training and awareness courses, we are rolling out a refresher to all team members at least annually to ensure that they remain alert and attentive to information security policies and procedures.

We also release quarterly ISMS Advisory to give constant reminders to all team members on how to be responsible in safeguarding the information assets of VBP.

What if a Team Member's device was stolen?

If a desktop (mini-PC) or laptop is stolen, the equipment is protected by hard drive encryption, ensuring that neither the drive nor any data on it can be accessed. The only action a thief could take is to reformat the hard drive, which would erase all data on it.

Is the team member's computer still protected against viruses, malware, or other attacks?

Yes, all VBP-issued equipment, including desktop (mini-PC) and laptops, are equipped with the same antivirus / endpoint / firewall protection software as when the team is in the office.

Are there procedures governing the printing of documents containing personal information?

To print team members' personal information would require drivers to be installed and administration access. So, unless authorised, printing or production of such information is not possible.

Can Team Members use web-based applications via their computer while working from home?

All websites accessed by team members are subject to scanning through our web filtering platform. Websites or web applications that do not meet established security standards are automatically blocked to ensure the safety and integrity of our systems.

If a team member encounters a blocked site that is essential for the completion of their tasks, a formal approval process must be followed to request access.

Please note that default restrictions remain in place for certain categories, including Gaming and Pornography.

Is there a Work from Home Security Matrix available that illustrates the extension of Policy and Security measures to the Work from Home setup?

Yes, the Work from Home Security Matrix is available upon request to VBP.

How is data encrypted on the Team Member's computer?

VBP employs a security feature to encrypt hard drives, ensuring that any files on them cannot be accessed without the encryption. This measure

secures data on desktop (mini-PC) and laptop computers, maintaining system integrity.

The encryption process requires team members to input multilevel log-ins when accessing their computers.

How do you manage passwords working from home?

VBP uses the same password management software when team members are WFH, as we do when the team members are in the office.

Further, there is a personal dashboard for the deployment and management of passwords. All sensitive information stored in the password manager is encrypted to ensure complete security and strong password generation for web and software applications.

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

Do you have a documented procedure for backing up data while Team Members are working from home?

VBP has an established backup and restoration procedure. This is to minimise the risks associated with data loss by defining a backup regime for all centralised VBP data services. This will ensure the safety and security of IT system resources and supporting assets.

All VBP data is backed up using cloud services and multiple platforms to provide redundancy. Various backup methods are employed depending on the data source and the importance of the information. The IT department follows an established backup schedule outlined in the procedure.

All data adheres to recoverable retention requirements, and any data stored in the VBP network is also backed up in physical storage.

Can Team Members access the USB ports when they are WFH?

Access to USB ports remains disabled for data devices, similar to the policy in place when team members are working from the office. USB ports are configured to only allow peripheral devices.

If a data device is detected and inserted, our security measures automatically block access to it.

Can Team Members install any software they want into their computer while working from home?

No, software installation requires an administrator password, just as it does in the office.

Software installation still follows the existing procedure and must undergo an approval and testing process.

Are there any Physical Security controls in place?

The physical security for WFH and WFP team members is, as can be expected, different to the VBP office.

While we do not have physical security controls in the homes of team members, as we have in the office (biometrics, CCTV, etc.), we nonetheless have protections in terms of:

- **Theft** – If a computer were to, for example, be stolen, this is a financial risk that is borne by VBP.
- **Data** – If a device was stolen or a third party sought to access it, we have encryption in place so the data is protected and could not be accessed.

In addition, we are directing team members to follow Standard Operating Procedures (SOPs) on how to protect data at work while they are working from home. This is stated in our Offsite Work Policy.

Signed and approved by:

Nathan Jacobsen
Chief Executive Officer

..... end