TREASURY WINE ESTATES

INFORMATION SECURITY POLICY

A Treasury Wine Estates Limited Policy

1. INTRODUCTION / CONTEXT

As one of the world's leading wine producers and sellers of premium wine, Treasury Wine Estates (TWE) handles a wide variety of information to operate its business. Information Security assists TWE with protecting information and assets from a range of threats, to maintain the confidentiality, integrity and availability of TWE information and resources, in order to minimise business risk and maximise business opportunities.

TWE management has adopted a risk based approach to identify key risks, threats and priorities. It is the responsibility of management to implement and maintain appropriate controls to minimise the risk exposure throughout the information systems lifecycle. These controls need to be established, monitored then reviewed and improved in conjunction with other business management processes on an ongoing basis.

The key objectives of the *Information Security Policy* are to:

- Ensure that all TWE information systems (including, but not limited to, all computers, mobile devices, networking equipment, software and data) are safeguarded to minimise the risks associated with the theft, loss, misuse, damage or abuse of these systems.
- Assure management that users are aware of, and comply, with all current and applicable legislation.
- Provide a safe and secure information system working environment for all TWE staff and personnel associated with TWE.
- Ensure that all users understand their responsibilities for protecting the confidentiality and integrity of the data that they handle.
- Protect TWE from liability or damage through the misuse of its Information Systems and IT facilities.

2. WHO THIS POLICY APPLIES TO

This policy applies to all permanent, temporary and contract employees of TWE (including any of its associated companies). This includes, but is not limited to, directors, agency staff, casual staff, contractors, consultants, and seconded staff ("associated persons") in all operations globally within which TWE operates.

3. POLICY STATEMENT

Confidentiality, Integrity and Availability should be safeguarded against a wide range of threats on TWE's information assets and resources to minimise business risks and ensure compliance with legal, regulatory, contractual and compliance requirements.

4. DEFINITIONS

Confidentiality	Ensuring that information is accessible only to those authorised to have access.
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Availability	Ensuring access to information and associated assets by authorised users, as and when required
DR	Disaster Recovery
BCP	Business Continuity Plans
CIO	Chief Information Officer
ITLT	IT Leaders reporting directly to the CIO

5. RESPONSIBILITIES

TWE Executive Leadership Team (ELT) and TWE Board	Owner of the security policy. Management delegates the responsibility for security-related documentation to the CIO. All changes must be approved and signed by the CIO.
CIO	Implement, Monitor, Review and Provide assurance of compliance with the Information Security Policy and report any significant information risks and breaches to the ELT. The CIO is also responsible for managing/updating this

	document and will review it annually or in the event of any change to TWE's strategy that may impact its risk exposure or technology requirements.
Business Managers	Accountable for the information asset and formally classify, comply, specify, monitor and review access controls, including any segregation of duties. Ensure changes to the assets are adequately tested and verify if the changes meet business requirements without negatively affecting any other asset or process. Responsibilities include: o Ensuring their staff are ware of TWE's obligations and their individual obligations in handling, processing and disclosing information correctly; o Taking appropriate action to report breaches or non-compliance with information security practices; o Embedding a culture that encourages the appropriate use of information and technology; o Ensuring that information and technology assets, critical to the business to operate are included in Business Continuity and Disaster Recovery plans; o Managing the lifecycle of information and information processing assets within their delegated area of responsibility; o Ensuring access to information and technology by staff is in line with their role and responsibilities.
Information Technology Managers	TWE's IT managers, analysts and project staff, (including management teams of third party providers or any contractors) have responsibility for complying and implementing controls to minimise business risks.
All Personnel	All personnel employed by TWE, including temporary employees, permanent employees, seconded personnel and those contracted by TWE, shall comply with TWE's Information Security Policy, manuals, standards and procedures.

6. POLICY

The following are principles for the management of Information Security for TWE and its associated partners.

- Information should be protected from unauthorised access and unauthorised disclosure.
- All staff must comply with TWE's Code of Conduct in the acceptable use of TWE information and technology products and services.
- Information security controls must meet the requirements of laws and regulations in the countries in which TWE operates and across borders.
- Licensing and Copyright obligations must be adhered to at all times.
- A security risk assessment must be completed annually to identify risks and mitigation plans or a change in business strategy/scenario.
- Awareness should be provided to all TWE staff, highlighting the importance of information security in TWE business operations.
- Breaches of information security, actual or suspected, must be reported to your line manager, the CIO or members of the IT Leadership Team (ITLT).
- Privacy of personal information belonging to TWE clients and held by employees, vendors and partners at TWE facilities should be safeguarded.
- Business Continuity plans must identify critical information assets, processes and technology dependencies to enable the development of Disaster Recovery (DR) plans.
- DR strategy must be built to address business risks and business impact occurring due to downtimes. Disaster Recovery plans must be documented, maintained and tested annually to ensure the recovery and availability of critical information assets.
- Agreements with third party users who handle TWE information must be in place allowing TWE to audit the controls in place to safeguard TWE information.
- Violations of information security policies or processes and non-compliance will be handled in accordance with TWE's *Disciplinary Processes Policy*.
- Information security policies should be reviewed and updated on an annual basis or following significant changes in the TWE business environment.
- All system changes must be logged, planned, assessed, documented, communicated, tested, authorised and supported during change to ensure changes on TWE assets are effective and does not cause major disruption to regular business operations. Additional policy and guidelines can be accessed in *IT Systems Change Management policy* and *Information Security Manual.*
- TWE Information assets must be classified in accordance with business needs and the impacts associated with those needs. The classification categories in use within TWE are "Confidential" and

"Commercial-In-Confidence". Where this requirement is not met, the information is deemed "Unclassified".

Confidential	Information is not in public domain and can be reasonable regarded as confidential or sensitive; or. Any other information given to you or comes to your knowledge during the course of your employment, that you are told or is labelled confidential or a reasonable person would expect to be confidential from its nature and content.
Commercial-In-Confidence	Information whose compromise could cause limited damage or uncertainty to TWE, its people, clients, business partners, customers, or members of the public. Information sharing is "Restricted" to specific groups. This may include external parties; however, confidentiality agreements must exist in order to share this information.
Unclassified	Information in the public domain where if information is disclosed, would not cause any damage or uncertainty for TWE.

- All personnel have an obligation to protect TWE's classified information by taking reasonable steps and necessary precautions to maintain the confidentiality and integrity of information by:
    - Not disclosing or sharing it with anyone except:
        - As required by law;
        - With the prior written consent of your manager or nominated business owner;
        - As approved and required by your job function.
    - Identifying classified information used by your team and making others aware of the degree of sharing permitted or special handling required to comply with laws and regulations.

7. VARIATIONS

Exceptions must be in writing submitted through the "Advanced IT – Risk Exception" Form via the TWE IT Request process. Requests will assessed for business requirements, circumstances and impacts on business processes with information or business asset owners. Compensating controls will be established as required in consultation and agreement with the business owner. All exemptions will be reviewed annually to validate the continuation of exemptions and to identify any need for policy, standards or procedural amendments

8. CONSEQUENCES FOR BREACH OF THIS POLICY

A breach of any of the provisions of this Policy may constitute a disciplinary offence and will be dealt with in accordance with TWE's disciplinary procedures. Depending on the gravity of the offence, it may be treated as misconduct and could render you liable to summary dismissal.

Any breaches of this policy must be reported immediately to your line manager and/or in accordance with the Whistle-blower Policy. Failure to report such breaches could expose TWE to an unacceptable level of risk.

Breaches or non-compliance by third parties will be handled according to terms and conditions contained in the relevant contracts between the parties.

9. RELATED TWE DOCUMENTS

This Policy should be read in conjunction with the following documents:

- TWE Information Security Manual
- TWE IT Systems Change Management Policy
- TWE Whistle blower Policy
- TWE Code of Conduct Policy
- TWE Social Media Policy
- TWE Document Retention Policy
- TWE Mobile Device Policy
- TWE Business Continuity Management Policy

10. APPROVAL

Approval of this Policy is required annually by the TWE CFO.

11. VERSION CONTROL

Last Edited by:	Policy Owner:	Date Published:
Marilou Bautista, Global Governance & IT Commercial Services Manager	Noel Meehan, CFO	July, 2016