TREASURY WINE ESTATES

INFORMATION SECURITY MANUAL

A Treasury Wine Estates Limited Policy

CONTENTS

1. INTRODUCTION

This manual should be read in conjunction with Treasury Wine Estates' (TWE) Information Security Policy and provides further detail supporting the policy requirements and achievement of policy objectives.

2. 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 who report directly to the CIO

3. INFORMATION CLASSIFICATION AND DATA HANDLING GUIDELINES

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. Information Classification and Data Handling will be monitored by Treasury Wine Estates (TWE) to classify and protect information by taking into account business needs for sharing or restricting information, as well as legal requirements. The classification scheme will include conventions and criteria for the review of the classification. The scheme will be consistent across TWE ensuring everyone classifies information and related assets in the same way. This also means that everyone has a common understanding of protection requirements and applies the appropriate protection.

Information classification status is defined as Confidential, Commercial-In-Confidence.

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.

1. Information must be labelled and handled according to its classification.
2. Electronic communications systems and all messages and data generated or handled by electronic communications systems including back-up copies, are considered to be the property of TWE.
3. TWE business records and other 'Classified' information must be regularly backed up, stored, and retained for the period specified by the TWE Document Retention Policy.
4. Back-ups procedure must contain a validation check to ensure successful copy of the required data, so it is available for recovery as and when required for business recovery purposes.

5. Classified TWE information must be destroyed, securely and permanently at the end of its lifecycle, including all backup copies.

4. IDENTITY AND ACCESS MANAGEMENT

Objective: To control access to TWE information by providing authorised users with access and preventing unauthorised access.

In order to maintain accountability, each user must be uniquely identified (UserID) with an identifier across all TWE systems.

1. Access to information systems and services is provided to individuals only on a 'need to know' basis (i.e. minimum privileges required to perform the job) and is based on job classification; function and segregation of duties defined by the information asset owner. This means that, by default, access is denied unless explicitly allowed.
2. Users must only access or attempt to access computer systems, applications, databases and files that they are authorised to access.
3. A formal IT user registration process, including appropriate approval by an Authorising Person must be in place for granting access to all information systems and services, and for subsequent changes to access permissions.
4. A user must not self-authorise requests. Authorising Managers must:
    - be a TWE employee with the delegated authority to perform this task, usually the user's line manager;
    - Understand the employment terms of the user, including their job function;
    - Validate the user's authenticity and rights to TWE information, assets and services.

The following table identifies out the Authorising Managers for various User categories:

Category of User	Authorising Person
Employees, TWE consultants or contractors, temp staff etc.	TWE Line Manager, TWE Application Role Approvers or someone in TWE Management with delegated authority to approve.
Third party suppliers, business partners or, IT Service Providers.	Nominated TWE business managers responsible for the contracts or as delegates appointed by the senior management team.
Executive TWE staff (ELT)	CEO, Chief Legal Counsel or Chief Human Resources Officer.

5. Responsibility for approving access to business applications and functions sits with the asset owner who is usually a business manager with day to day responsibility for the business process that the application supports.
6. Access privileges of employees must be reviewed annually by the Authorising Person, to ensure that access is still appropriate and consistent with the requirements of the job function.
7. The IT Services Team will maintain a list of business managers responsible for approving access to information systems which may be different to the user's line manager. The list should be reviewed and updated every six months.
8. Administration for provisioning and de-provisioning of access rights should be centralised. The responsibility for performing this activity for individual systems and applications can be delegated, provided business access rules have been clearly defined based on, job roles and responsibilities.
9. IT Access Request to information systems and services must be logged for:

- New users
- When a user's job role changes.
- When a user leaves TWE

10. TWE's Human Resources function must advise the IT Service Desk of the effective termination date of an employee in a timely manner. UserID's will be disabled and then removed as soon as possible after the termination of the user's employment or contract. Remote network access capability will be removed immediately if it is not critical to performing the particular job function.

11. The assigned UserID and password combination should be used to provide access to all approved TWE information resources, unless technical or other limitations prevent it or the security of the password management system on a specific resource does not meet TWE standards.

12. 'Group' or 'Generic' UserID's are used in exceptional cases. Their purpose must be documented and approved by submitting a Risk Exemption form. Responsibility for a Generic UserID must be given to a named TWE manager, who is responsible for approving usage and all actions perform by the UserID. They are also responsible for removing individual users and reviewing activities performed by the account. Another compensating control includes keeping and actions taken where anomalies are discovered.

13. Computers, terminals or applications, should be logged off when unattended or not in use. Locking mechanisms, such as screen locks, should be invoked when temporarily away from your desk or when idle.

14. Screen savers should automatically activate after 10 minutes of inactivity.

15. Vendor-supplied default user accounts and passwords must be changed and unnecessary user accounts eliminated as soon as practical after installation but before systems are installed on the TWE production network.

16. Development and test IT environments must maintain controlled access. Activity should be logged to ensure that only authorised activity is conducted.

17. Redundant UserID's must not be issued to other users.

18. When a UserID is not used for a period greater than one month, the UserID must be locked or disabled to prevent anyone using it. When the UserID is required again, it can be re-enabled. Examples of this situation include employees departing on maternity leave or other extended leave of absence. Individuals or the Line Manager must notify the IT Service Desk in advance of the period of absence so that the UserID can be disabled and enabled accordingly.

19. When a temporary UserID is required, for example a contractor working on a specific project, the UserID should be set to automatically disable at the end of allocated time period. Should it be subsequently required for a further period, the deactivation time should be extended.

20. 'Special' or 'Privileged' task-related' accounts, often referred to as 'service or system accounts' are used by IT Infrastructure and many applications run system tasks. By default, they are highly privileged accounts and knowledge of these accounts must be restricted based on job functions. These accounts should not be used for any operational activities.

21. A register of 'Special' accounts must be centrally managed by the IT Governance Team. Changes to these accounts must be strictly controlled. The UserID and password for these special accounts must be securely recorded, stored and should be available in case of an emergency.

22. 'Special' accounts such as administrator, root or equivalent database and application accounts must utilise stronger authentication techniques, such as longer passwords, one-time use only passwords, two-factor authentication or digital certificate authentication mechanisms.

23. A six monthly review of Special or Privileged access UserIDs should be performed by the respective business manager to ensure: access rights are authorised, unauthorised privileges have not been allocated and that all changes to privileged access accounts have been logged.

24. System routines or programs capable of running without privileges should be developed and used wherever possible. These routines should also be used to avoid the need to grant privileged access to users.

25. Administrators must only use their administrator UserID or 'Special' accounts for administrator functions and their named UserID for non-administrator activities. Use of UserID descriptive or generic names, such as 'administrator' or 'supervisor' should be changed wherever possible to avoid exploitation.

26. New users will initially be provided with a secure temporary password which must be changed immediately. Temporary passwords provided when users forget their current password will be supplied by the IT Service Desk, but only after a positive identification of the user.

27. Password standards are maintained in PPE (Password Policy Enforcer) and/or GPO (Group Policy Object) in AD.

28. Passwords must be kept confidential and must not be disclosed or shared with others. Passwords must not be displayed on the screen when entered. Complete passwords must not be recorded or displayed where others can see or access them. This includes in log files or audit trails.

29. Passwords must be stored in an encrypted form separately from application system data and must be transmitted across any networks in protected form (encrypted or hashed), unless it is technically infeasible to implement. In these cases an exemption to policy must be submitted, so the risks can be assessed.

30. Automated processes must not include passwords (e.g. stored in a macro, function key, auto entered).

31. Mechanism to prevent the capturing of logon credentials must be employed wherever possible.

5. INFORMATION TECHNOLOGY (IT) ASSET MANAGEMENT

Protection of TWE's IT Assets is necessary to reduce the risk of unauthorised access to data and to protect against loss or damage of TWE's physical Information assets.

Information processing assets include:

- Desktop or notebook computers and mobile devices (e.g. iPhones, iPads etc.);
- Information processing servers, such as file and print, database, mail and application servers and operating systems (e.g. UNIX, MS Windows, etc.);
- User authentication devices, such as tokens, smart cards and biometric terminals;
- Telephony and audio-visual equipment and services including voicemail, audio/video conferencing, cameras/video etc;
- Peripheral devices (e.g. printers, multifunction devices etc.)
- Network devices and data carriage services (e.g. firewalls, routers, switches, internet services)
- Data and information contained in and processed by TWE application systems or support and training documentation
- Storage media, including backup devices and storage media, such as tapes.
- Integration systems such as A2A, B2B and ETL

All IT assets remain the property of TWE and due care must be taken to protect the physical asset and information stored in it. For example, "care" means ensuring that data is regularly backed up, assets are kept away from harm and passwords are secure.

1. The security of IT assets rests with the individual who has been assigned custody of that asset. He/she is responsible for ensuring that all reasonable care has been taken to protect TWE information and for its physical security.

2. Responsibility for the security of authentication devices, such as tokens and smart cards rests with the individual who has been assigned custody of the device.

3. Portable IT assets must be protected against theft, particularly when removed from TWE premises. Specifically, IT assets:

- must not be left unattended in public ;

- must be carried as hand luggage and disguised where possible when travelling;
- must be secured with a locking cable and/or locked when not in use and after business hours;
- must be subject to due care when used at home, considering issues such as access by non-TWE employees including family and friends.

4. Confidential information must not be held in portable computing equipment unless TWE approved protective mechanisms (e.g. power-on password or file encryption) are in place and active.
5. Physical assets / devices must have TWE classified information permanently removed or deleted when the asset changes ownership, is at the end of the device life, or if lost or stolen.
6. The currency of anti-virus and malicious code protective measures must be maintained and not disabled.
7. Any IT asset lost or stolen must be reported immediately to both the employee's manager and the IT Service Desk. The Police should also be advised if it is believed a crime may have been committed.
8. Particular care must be taken when using the equipment (TWE assets like laptops and portable devices) in public locations, such as in aircraft, waiting areas and client or third party offices so that strangers cannot observe the contents of the screen. A password-protected screen saver should be invoked when the equipment is powered-on but not in active use.
9. An appropriate data backup strategy must be developed and followed. This should include selection of the source data to be backed up, frequency of backups, backup media, storage location and periodic testing of the data restoration process.
10. All IT assets must be returned to TWE when leaving the organisation, or upon request, which may be either verbal or written.
11. If an employee fails to return an IT asset or does not provide an acceptable explanation as to why the asset cannot be returned, the employee may be charged for the cost of that asset and his/her future access to TWE assets will be reviewed.
12. IT assets acquired for TWE business purposes must be selected from a TWE Approved IT Products List, unless prior authorisation has been obtained from the TWE Infrastructure Manager. The approved product list should include a statement about acceptable uses and the procurement process to enable license tracking.
13. An inventory of all IT assets must be maintained. The inventory should include details of the asset, its custodian and the personnel authorised to use the asset. Devices should be labelled with custodian, contact information and purpose.
14. Equipment provided by TWE must not be altered in any way, for example by upgrading processors, memory or other features, without prior authorisation from the TWE Infrastructure Manager. Requests should be submitted via the IT Service Desk and will be implemented by the IT Department.
15. Outside of business hours all desktop and notebook computers should be logged out of the network and applications, however the equipment should be left powered-on. This will enable the equipment to receive automatically downloaded software and system updates.
16. All computer systems, including desktop, notebook, midrange and mainframe, must be configured, installed and maintained in line with the appropriate TWE platform build standards that address known security vulnerabilities and good practices.
17. Appropriate early warning and alerting services must be monitored to identify the latest system security vulnerabilities. Vendor supplied security patches must be tested and where applicable, installed.
18. The clocks and times of all computer systems on the TWE network must be synchronised with an agreed, accurate and reliable time source using a robust protocol such as NTP.

6. COMPUTER SOFTWARE ACQUISITION AND USE

TWE is committed to providing sufficient legitimate software to meet business needs and consequently, there is no need to use unlicensed or otherwise illegal software. Licensed and registered copies of software are acquired from a variety of sources. These are installed on computers within TWE and appropriate backup copies are made in accordance with the licensing agreements.

TWE reserves the right to protect its reputation and its investment in computer software by enforcing strong internal controls to prevent the making or use of unauthorised copies of software. These controls may include periodic assessments of software use, announced and unannounced audits of company computers to ensure compliance, and the removal of any software for which a valid license or proof of license cannot be determined.

1. Software installed and/or used on TWE IT systems must be legally acquired by TWE.
2. Software acquisition must meet Procurement Policy and procedural requirements to ensure copyright and licensing obligations are understood and met.
3. Approved software must be certified for use on the TWE Standard Operating Environment.
4. Freeware or software obtained free of charge, must not be installed on TWE devices unless it is approved for use in a corporate environment. Advice should be sought from TWE legal department to understand TWE's obligations.
5. The following controls should be implemented to ensure compliance with software copyright laws to ensure appropriate evidence of this compliance is readily available:
    - A register of approved software and agreements must be maintained, together with the number of users;
    - Original media (diskette, CD-ROM etc.) must be stored securely;
    - Licenses must be returned to the pool when the software is no longer required;
    - Audit of software licensing should be defined and undertaken.
6. Software that provides encryption capability must meet TWE's encryption standards and be specifically approved by the IT Operations or Technical Services team before being installed on any TWE systems.
7. Software and any associated documentation and data must be securely removed from any device when the asset changes ownership, is disposed, or at the end of its useful life.
8. A robust process must exist to ensure that only approved versions and configurations of software is implemented by staff responsible to perform this task.

7. PHYSICAL AND ENVIRONMENTAL PROTECTION

Business information processing assets should be housed in secure areas. If physical security controls are inadequate, the best and most sophisticated logical access controls can be circumvented by directly accessing computer hardware and software media.

Information processing facilities are identified but not limited to data centres, computer rooms, server rooms, network and hub rooms, wiring closets, PBX rooms, PC's, laptops, servers printers and any other equipment needed for the functioning of TWE IT systems..

Equipment must be protected by defined physical security perimeters with appropriate barriers and environmental controls in place.

1. The design of secure facilities must be based on a risk assessment that considers appropriate environmental and physical controls to limit and monitor access. Video cameras and motion detectors can be considered as a control, to monitor entry and exit points in high risk areas.
2. Computers and network equipment must be housed in a secure facility with access restricted to personnel based on their job responsibilities.

3. Computer and computer storage areas must provide and ensure protection from environmental elements such as heat, dust, smoke, fire, water, humidity etc.
4. Computer and network room doors must be equipped with a locking mechanism, which allows only authorised personnel access. Keys or electronic access cards must be controlled to ensure that only authorised personnel have access.
5. Keys and access cards must be kept secure at all times. Never lent to contractors, visitors or other employees, and must be returned when finishing employment with TWE. When access cards are used, each access (and if appropriate exit) must be logged and this log reviewed on a regular basis by management.
6. Visitors to computer and network rooms, including vendor representatives and maintenance personnel, must be registered and must carry appropriate identification. A TWE employee must accompany non -TWE visitors to secure areas at all times.
7. Where possible, multi-function devices, printers, or facsimile machines that receive or send classified information messages must be located in a secure area, or utilise security features, that restricts access to authorised personnel.
8. High availability facilities, such as data centres must have automatic incident alerting established to fire departments, telecommunications providers or emergency services as appropriate.

8. NETWORK, REMOTE ACCESS AND MOBILE SERVICES

Remote access connections extend the corporate network and are a primary source of uncontrolled points of access to the network. A higher level of security needs to be applied to these connections.

Key threats for remote access management are to guard against:

- Loss, damage, unauthorised disclosure or theft of business information
- Unauthorised access or changes to internal systems, particularly to sensitive or critical business systems, or misuse of any TWE information processing facilities.
- TWE employees accessing business partner systems and information must use caution and ensure that they act in accordance with TWE and business partner policies

Unauthorised and insecure connections to TWE's network services can adversely affect the whole organisation. TWE must ensure that access to TWE computer networks and systems from sources outside the TWE perimeter (e.g. from the internet or via an external connection such as a business partner network connection), have appropriate controls in place

1. Access to TWE's network and remote access facilities must be controlled and must be based on a risk assessment.
2. All configuration changes to network infrastructure, including firewalls, routers, switches or appliances etc. must comply with TWE Change Control procedures, following formal approval and testing.
3. Remote access to TWE network via any connection, (VPN, wireless, ISDN or vendor provided dial-up services etc) will be provided on a needs basis and must use the approved TWE network facilities with strong authentication.
4. Multi-factor authentication or a challenge response mechanism must be used to validate the authenticity of the user.
5. All requests for remote access connections to TWE network must be approved by the appropriate authorising person before access is granted.
6. Details of all remote access attempts must be logged and logs maintained for at least twelve months. The logs should include login attempts whether successful or not, with as much information as deemed necessary about the source of the attempt.

7. When mobile devices are connected to the TWE internal network via a LAN connection, all external connections must be disabled.
8. External or remote connections to TWE desktop or server computers must have a business justification and must be authorised through the IT Risk Exemption process prior to the connection being permitted. Authorised connections to these systems should be configured to allow only outgoing connections. In this situation, the ability to establish an incoming connection from an external source must be disabled by system configuration options. Where authorised connections need to be configured to receive incoming connections for clear business benefit, compensating controls must be in place, such as only activating the connection when needed and deactivating immediately after use.
9. Remote network connections / sessions should automatically disconnect after a specific period of inactivity.
10. IT assets not supplied by TWE must not be connected to the TWE corporate network without prior written approval, achieved by using the TWE Exemption Process. This includes computers and network components, such as wireless networks or equipment used by visitors or third parties during meetings.
11. Authorised wireless networks must be implemented with all relevant security options enabled to prevent unauthorised access or surveillance of the network.
12. All users of wireless networks must be formally registered using a defined process.
13. When devices with wireless network adapters are connected to the TWE internal network via a LAN connection, the wireless network adapter must be disabled and not used.
14. All internet access points must be monitored, logged and reviewed to prevent and / or detect security incidents. High risk events should trigger alerts to technical staff, to automatically notify them of these events.
15. All client access points (WAN connections, VPNs, business to business connections etc.) must be formally requested through the standard approval process and follow change management procedures where appropriate. Only authorised connections and activity are permitted. Activity must be logged and reviewed weekly by technical staff to identify anomalies. High risk events should be reported to IT Risk and Security Manager.
16. All classified information transmitted across public networks must be adequately encrypted to maintain its integrity and confidentiality.
17. All non-console administrative access to midrange systems, must be adequately encrypted using technologies such as SSH, VPN or SSL/TLS.
18. All TWE supplied mobile equipment must have TWE approved security protection functions installed, configured and running at all times. Users must not disable or reconfigure the security mechanisms unless specifically instructed by IT Technical staff. Additional policy and guidelines can be accessed in *TWE Mobile Device Policy*.
19. Wherever payment cardholder data (refer PCI Data Security Standard) is accessed remotely, the accessing device must be configured so that cardholder data cannot be stored on local hard drives, portable storage media or other external media. In addition, cut-and-paste and print functions must be disabled.

9. VIRUSES AND MALICIOUS CODE

Software and infrastructure are vulnerable to malicious software, such as computer viruses, network worms, trojan horses and logic bombs or other automated forms of attack. These can enter an organisation via many access points and devices available, such as: IT media (USB sticks, CD-ROM's, or DVD's), email messages (including attachments), portals or remote connections across public or private networks. New threats appear on a regular and continuous basis and therefore rigorous processes need to be established to ensure the management of viruses and malicious code from entering the TWE environment.

1. Anti-virus and malicious code detection software must be installed on all eligible IT systems and its currency maintained.
2. All electronic information introduced to the environment from external sources, including: the internet, USB sticks, CD/DVD's, attachments to email messages and downloaded files must be scanned for viruses and malware before use.
3. The anti-virus and malicious code detection software, its settings, parameters and general operation must not be altered or disabled.
4. Vendor supplied patches that address vulnerabilities must be tested and applied as early as possible after vendor release.
5. TWE IT team who manages Operations or Technical Services will distribute and maintain the latest available software upgrades, anti-virus software and virus signature files.
6. Actual or suspected virus infections must be reported to the IT Service Desk, regardless of whether the infection is believed to have been removed or not. The IT Service desk must respond to all reported virus infections to ensure that all instances are eradicated from local systems and administrators of remote and non-TWE systems are alerted.
7. The IT Service Desk must report monthly on incidents relating to virus and malware activity.
8. Appropriate early warning and alerting services must be monitored to identify the latest system vulnerabilities. Appropriate action should be taken when new vulnerabilities are discovered, to prevent the exploitation of the vulnerability.
9. Viruses and other malicious code must not be created or executed/transmitted across the TWE IT infrastructure. This includes maliciously or intentionally changing or deleting files to stop a computer from operating as expected.
10. Identification and prevention of virus and malicious software threats should be included in user security awareness initiatives.
11. Details of abnormal virus and malicious code events must be securely logged and the logs retained for an agreed period.

10. ACCEPTABLE USE OF INTERNET, EMAIL AND SOCIAL MEDIA

TWE trusts its staff to act responsibly, to be ethical and be efficient in their use of TWE's resources and services. This responsibility includes the use of electronic media such as the internet, email and social media. TWE also has a responsibility to protect its employees from harassment, vilification and exposure to unethical or immoral internet and email content.

The use of the internet for business purposes is widespread with significant benefit resulting from the quick and easy access to the vast amounts of information. Since the internet is an open, public network with limited overall management controls or framework, special care must be taken in assessing and managing the inherent risks before it is used by TWE. Additionally, the use of email and social media forums are subject to laws and regulations to which TWE and its staff must comply. Email is subject to the same laws as any other form of correspondence, including statutory record keeping requirements and can be subpoenaed or 'discovered' during legal processes. Social media require staff to disclose their employment with TWE. Key guidelines and requirements are as defined below.

1. Access to the internet and email facilities is provided primarily for business purposes. Incidental personal use is permitted, such use does not impact on TWE operational needs.
2. It is unacceptable to intentionally create, send, access or store information that could damage or embarrass TWE, its employees or its clients. Each person is responsible for ensuring their use:
    - Does not consume more than a trivial amount of TWE resources;
    - Does not interfere with worker productivity;
    - Does not impair the reputation of TWE with your online presence and views.

- Is not offensive to others and is in line with TWE values;
- Is not used for personal gain or the advancement of individual views;

3. Personal communications should not be assumed to be private and employees may not have the same personal and privacy rights as they would using when using their personal computers. TWE respects the privacy of its employees and will use its best endeavours to protect legitimate personal communications against disclosure.
4. Access to the internet must be via TWE approved network paths and protective mechanisms.
5. Use of TWE logos, trademarks or domain names utilised for TWE official business must be approved by Director for Intellectual Property.
6. TWE reserves the right to monitor internet and email usage to ensure compliance with all relevant policies and applicable laws.
7. Software must not be downloaded from the internet or installed on TWE resources without appropriate approval from authorised TWE IT Representatives. See Section 6: Computer Software Acquisition and Use.
8. TWE computers must not be used to gain or attempt to gain illegal access to other computers or networks (i.e. hacking/cracking).
9. Use of electronic services such as the internet and email must be in accordance with applicable laws and used for TWE's business purpose. However personal use is restricted.
10. Material received inadvertently that is unacceptable or inappropriate must be immediately deleted from TWE systems. Such material must not be forwarded.
11. A user's identity on an electronic communications system must not be misrepresented, obscured, suppressed or replaced. The user name, electronic mail address, organisational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.
12. The origin of messages must be independently validated before actioning an email instruction, to enter into a legal transaction on behalf of a customer.
13. Confidential or client-sensitive documents, such as personal or health information must be transmitted via a secure mechanism and should not utilise the email system unless TWE approved protective mechanisms such as encryption are in place.
14. Business conducted using email must be documented to meet legal, operational, audit, legislative or other internal requirements. This includes archiving and retrieval of documents and emails when necessary, which remain the property of TWE.
15. Files attached to email messages or downloaded from the internet must be automatically scanned with virus detection software before installation, opening or processing.
16. Internet connections / pages must be scanned for malicious content prior to opening.
17. Where email communications form part of official records, they should not be deleted and should be attached to official files, according to business practices and TWE Document Retention Policy.
18. Email communications sent by individuals may not reflect the views of TWE.
19. Official disclaimers should be attached to outgoing emails to ensure that unauthorised communications are identified as expressing the views of the sender and not necessarily the views of TWE.
20. A Logon Disclaimer must be presented to users at the time of access, to identify the ownership of the environment as TWE's and to reiterate the appropriate use of TWE computer facilities and services.

11. SECURITY INCIDENT HANDLING

With the ever growing requirement for information sharing and the trend towards greater networking, it is important that information security incidents are reported, analysed and actioned quickly to minimise the impact of such incidents.

Security Incident handling procedures assists TWE in managing incidents such as fraud, hacking, proliferation of malicious software, other malicious acts, accidents, weaknesses in procedures etc. A comprehensive action plan is required to minimise the impact of the incident and prevent their recurrence.

1. All actual or suspected security incidents or system security weaknesses must be reported to the IT Service desk immediately or can be reported to your manager or according to the Whistle-blower policy.
2. If a TWE user is aware of an information security incident then they must report it to the IT service desk.
3. A process should be in place to establish, document and communicate security incident response and resolution, including escalation procedures, investigation of security incidents and logging details of findings for subsequent review.
4. Security Incident reporting relating to viruses must form part of the IT Service Desk monthly Security reporting metrics.
5. The content of any message or piece of information about a security incident that is intended to be released to the public or the media must be authorised by the TWE Corporate Affairs Team prior to its release.
6. Evidence relating to a security breach must be collected to comply with statutory, regulatory and contractual obligations. If action is likely to be taken against a person or an organisation, advice should be sought from TWE's HR department or legal advisers at an early stage in the incident handling process. In particular, any IT asset or supporting reports or logs should be physically and logically secured so that they can be preserved as evidence and cannot be tampered with or accessed remotely.
7. TWE will comply with its responsibility to notify the Police if it is reasonably believed that a criminal offence has been committed.

12. AUDITING, MONITORING AND COMPLIANCE

TWE reserves the right to monitor, copy, access, audit, remove or disclose any information or files that are stored, processed or transmitted using TWE equipment and services. TWE may monitor the computing and communications environment on a random or on a continuous basis to:

- Prevent the computing environment from being compromised by malicious code or software;
- Ensure compliance with laws and regulations by preventing the downloading of unauthorised software;
- Investigate conduct of operational activities that may be illegal or could adversely affect TWE its employees or its business partners;
- Prevent inappropriate use of TWE systems, networks or information.

Key Guidelines are as below.

1. Security logs and audit trails will be produced to monitor the activities of users in their usage of IT systems and services.
2. Exception to policy must be recorded and include: a business justification for the request, an assessment and analysis of the risk, any compensating controls implemented and approvals for the acceptance of the residual risk.
3. High risk tasks must be identified by business process owners. Activities performed against these tasks must be recorded in logs and produce audit trails. Alerts should be sent when exceptional activities are performed, when thresholds are reached or critical events are triggered. These

should be securely stored for an agreed period to assist in future investigations and access control monitoring.

4. Audit trails must exist to assist with accurately identifying by time and date, objects that perform cross system activities to subjects. This must include the source and destination subject or computer system identity, time and date stamps, processes or tasks performed and level of activity (read, write, delete).
5. A review of exceptional activity must be performed on a regular basis by managers, to detect any attempts to breach information security. Software tools may be used to filter log files to produce exception reports.
6. Critical system events requiring high priority attention must be identified and monitored. IT operational staff must be alerted immediately to ensure these events are controlled and managed.
7. Access to log files and audit trails must be restricted and controlled. They must be stored securely so that modification by any user is not possible. For longer term storage, logs should be transferred to write-protected media. The use of file integrity monitoring and change detection software should be considered.
8. All activities undertaken in the allocation, modification and revocation of user access must be securely logged using manual and electronic processes as appropriate.

13. SYSTEMS DEVELOPMENT & MAINTENANCE

Information Security must be an integral part of the development and implementation of new systems. When business requirements are identified and designed, security requirements must be formulated, corresponding to the sensitivity and availability of data to be handled by the system. Development tasks may be performed in house, or contracted/temporary resources, be outsourced to a contracted third party or a combination of these alternatives.

Maintenance for all system modification must be controlled and performed in a manner that does not impact business operations. System can be at risk if maintenance is not applied to systems in a consistent and controlled manner. .

The policies in this section apply regardless of how the systems development or maintenance activity is carried out.

1. All proposed systems development must be supported by a business justification. Ownership and responsibility for the development will ultimately rest with the business owner of the system.
2. Before a new system is developed or acquired the business owner must specify the relevant security requirements as part of the business requirements. These will normally be identified as the result of a formal risk assessment activity.
3. All system development and software maintenance activities must subscribe to IT Project Management processes to ensure consideration is given to relevant TWE policies, standards, procedures and other system development conventions.
4. In the absence of special management approval to the contrary, all software development projects must use mature, commercially available development tools and techniques that have undergone significant scrutiny and use in the public arena.
5. Separate test and production environments must be maintained. Preferably the environments should be physically isolated but, if this cannot be justified then the environments must be logically isolated and access control implemented.
6. All implementations of new systems and changes to existing software and applications must follow TWE's IT Systems Change Management policy and procedures. This must include user acceptance testing, communications to users impacted by the changes and formal hand over to support procedures.

7. If operational data containing personal or sensitive information is copied to create test data then the data must be depersonalised or desensitised before use in another environment.
8. Operational and developmental system documentation must be produced prior to the system's release into production and the documentation maintained. The extent to which a system is documented, will depend on its criticality to the business, its life expectancy, sensitivity and integrity requirements of the data it is processing and the complexities, including interfaces and other system inter-dependencies.
9. Strict control must be maintained over executable code and program source code.
10. Programs and data files conceived, developed or created using TWE equipment, information or time, are considered to be the property of TWE and protected by copyright unless otherwise agreed in writing.
11. Prior to any system or application being released into production it must meet security requirements by testing implemented system controls.
12. Appropriate controls must be maintained over external resources, such as consultants and contractors who perform systems development activities on behalf of TWE.
13. Appropriate security controls and audit trails must be designed into application systems. These should be determined on the basis of security requirements and a risk assessment and could include cryptographic systems and techniques.
14. All systems, files or applications for critical business functions, should utilise server- based storage and not the local drive of workstation computers.
15. Original TWE software media should be stored in an IT approved Software Repository, so it is available for recovery purposes.
16. A project request must be completed and submitted to the IT project management office, to initiate IT engagement in the development, maintenance and support of an application.
17. All IT project management processes must be followed through the project lifecycle, to ensure governance over the system development process.

14. THIRD PARTY ACCESS AND OUTSOURCING

TWE information might be put at risk due to access required by third parties. Third parties may act on behalf of TWE or may require access to, or from TWE environment, in order to provide a product or service. TWE may also unknowingly introduce risks into inter- organisational processes if a high degree of outsourcing is applied or several parties are involved in providing products and services.

Third parties cover different external party arrangements. Examples include: service organisations, an individual contractor or temporary employee, an agency, customer or supplier etc. Where there is a business need for working with third parties (also referred to as external parties), a risk assessment should be carried out to identify any security implications and control requirements. Consideration should be given to the third parties' Information Security Management practices and protection of TWE information assets, partially where information integrity can be put in doubt, confidentiality compromised, personal data transferred, or where information facilities are not available to TWE as and when required for normal business operations.

1. Permission for access to and use of any TWE information by a third party must be controlled based on a risk assessment, must be approved by TWE business managers and governed through clauses built into agreements and contracts reviewed by Group Legal, Global Procurement and the ITLT Sponsor to ensure compliance with laws and regulations.
2. Third parties must sign a standard contract and statement of confidentiality or non- disclosure agreement, which confirms their adherence to TWE's information security policies and advises penalties for non-compliance. For example, it should allow for termination of the agreement and recovery of expenses by TWE if security, confidentiality or other policies are breached.

3. Access must not be provided until the appropriate controls are implemented, with a signed contract defining the terms and conditions for the working arrangement.
4. Right to audit is a requirement of all third party agreements.
5. Compliance with TWE's Information Security policy and standards must be defined and included in agreements and contracts. As a minimum, agreements should cover the need for the third party to:
6. Comply with TWE policies and standards, including IT Project Management procedures, IT Systems Change Management procedures, Secure access requirements, Data retention and disposal requirements, and privacy legislation as it applies to TWE.
7. Provide TWE ELT evidence of compliance with PCI (Payment Card Industry) Data Security Standards annually, where applicable;
8. Submit to TWE auditing procedures to measure compliance and to provide assurance with TWE's internal controls;
9. Define processes for validating and terminating physical and logical third party user access to TWE information and information processing facilities;
10. Provide evidence of: certification with SSAE16 – Service Organisation Control Reporting or similar independent testing of security controls, where the party is performing a Data Centre Service Provider role on behalf of TWE.
11. Business processes involving external parties should be identified and appropriate controls implemented before granting access.
12. Privileged access required to perform activities must be managed and monitored by the third party to ensure access is commensurate with job function.
13. Third Parties must ensure their staff are aware of their compliance requirements and TWE's information security requirements.
14. Defined contingency plans should be in place at external and third party sites upon which TWE has a significant dependence, such as major suppliers and vendors. TWE should ensure that provisions are made in agreements for plans to be tested annually or in accordance with an agreed schedule.
15. A risk assessment must be performed to identify the impact of access not being available to the external party as agreed in the contract.
16. External parties receiving inaccurate or misleading information must report this immediately to IT Service Desk.
17. Where the external party is entering information into systems on behalf of TWE, clauses in contracts should ensure a high degree of data integrity and data quality. Where possible processes should be automated.
18. Where software development is outsourced, important aspects such as code ownership, intellectual property rights, rights of access to audit the quality and accuracy of the work performed, must be included in the contract between the parties.

15. DISASTER RECOVERY MANAGEMENT

Business Continuity and Disaster Recovery Plans are essential for the continuation of key business services in the event of a disaster or crisis which seriously disrupts normal business processes. The successful recovery of business systems and information following a disaster is directly dependent on the extent to which the business continuity and recovery has been planned. The plans should include measures to identify and reduce risks, limit the impact of threats and ensure a timely resumption of business services.

1. Data backups must be given an appropriate level of physical and environmental protection, including storage at an offsite location, consistent with their importance.

2. Business and IT operations manuals should define recovery procedures including Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
3. Authorisation to restore data from backup media and overwrite existing production data must be obtained from system and data owners. Written authorisation can be delegated to the Crisis Management team and / or assumed under certain circumstances in consultation with business managers.
4. All movements of backup media must be monitored and logged. The movements to offsite storage must be via a secure courier service. The contents of the onsite and offsite backup stores must be audited on a periodic basis.
5. The Business Continuity Plan (BCP) must identify and specify the requirements for the recovery of IT systems and services that provides the basis for the disaster recovery plan.
6. A Disaster Recovery Plan (DRP) must be developed and maintained and be readily available for the recovery of the TWE IT environment following a disaster or crisis. This plan shall be in compliance with the TWE Business Continuity Plan.
7. Employees must be made aware of their own respective roles in the DRP.
8. The DRP must be periodically tested to ensure management and employees understand how the plans are to be executed, including availability of key personnel and communication with support groups.
9. Backup copies of the DRP must be held securely, but must be easily accessible in the event of a disaster.
10. Critical business information, including documents, spreadsheets, presentations and plans created on personal computing equipment, business email messages and attachments must be stored on network servers. This will ensure that the information is appropriately backed-up and is available to others in TWE in a crisis situation.

16. 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

17. APPROVAL

Approval of this Manual is required annually by the TWE CIO.

18. VERSION CONTROL

Last Edited by:	Owner:	Date Published:
Marilou Bautista, Global Governance & IT Commercial Services Manager	Ash Peck, CIO	July, 2016