

RESORTS WORLD™ SENTOSA	BUSINESS UNIT: IT	EFFECTIVE DATE: 1 Jan 2026
	TYPE: POLICY	DOC REF: IT-P(E)-001

**IT End User Policy
Version 2026-1**

RWS Restricted

Revision History

Version No.	Effective Date	Section Amended	Reason for Change
2019-1	1 Jan 2019	- Added clause 5.1.11 on IT Security awareness training - Added clauses 5.3.2, 5.5.9 & 5.6.2	Alignment with new control requirement from CIS ICC clause 2.2. Enforcement of new IT Security controls
2019-2	31 Oct 2019	Amended clauses 5.7.1 & 5.7.2 - inserted a more detailed description	Document updated after review.
2020-1	15 Jun 2020	- Amended clause 5.1.10 to include the Personal Data Protection Act - Added clause 5.1.12 to include the Data Governance Policies	Document updated after review.
2021-1	31 Dec 2020	Amended clauses 5.1.6, 5.1.11, 5.3.1, 5.3.6, 5.3.9, 5.5.1, 5.5.9 and 5.6.1 for better clarity	Document updated after review.
2023-1	01 Jan 2023	- Updated 5.1. Acceptable Use - Summary of Reference to Authority Regulations	Updated 5.1.12. Users shall adhere to the following data governance policies: i. Data Management Policy ii. Data Security and Classification Policy iii. Data Incident Reporting Policy Rename "CRA" to "GRA" Updated the RWS logo
2023-2	21 Apr 2023	Added User Acknowledgment page	Added User Acknowledgement and Sign off page
2024-1	1 Jan 2024	Added 5.2.8, 5.2.9	Added clauses to password management
2025-1	1 Jan 2025	Added 5.5.11	Added clause on the use of Group assigned email address for non-business purpose.
2026-1	1 Jan 2026	Amended clauses 5.3.3, 5.3.9, 5.3.10, 5.5.5, 5.5.11, 5.6.7 and 5.8.1 for better clarity	Document updated after review. Added

** Minor changes such as rewording are not reflected in this change history table*

RWS Restricted

Distribution List

1) All	

Summary of Reference to Authority Regulations (If applicable)

Ref #	CCA/Reg/ICC/GRA Direction Description	Effective Date	SOP/Policy Section
CIS ICC 2.3 IT ICC 02.2	All users of IT systems receive IT security awareness training relevant to their job function. This training is conducted at least once a year. The training also covers the familiarisation of the Acceptable Use Policy	30 Aug 2022 02 Aug 2022	All

Contents

1. INTRODUCTION	5
2. OBJECTIVE.....	5
3. SCOPE	5
4. ACRONYMS.....	5
5. POLICY	6
6. DISCIPLINARY ACTIONS	8
7. IT END USER POLICY ACKNOWLEDGEMENT.....	9

RWS Restricted

1. INTRODUCTION

The IT End User Policy applies to all users within Genting Singapore Limited, Resorts World at Sentosa Pte. Ltd., Genting Integrated Resort Operations Management Pte. Ltd. and any other company that may come under the management oversight of Genting Singapore Limited presently and/or in the future, including all their subsidiaries, affiliates and overseas offices (collectively referred to as the “Group”).

2. OBJECTIVE

This policy sets the terms to govern the proper usage of the Group’s IT systems.

3. SCOPE

This policy applies to ALL users of the Group’s IT systems.

4. ACRONYMS

Term	Definition
RWS	Resorts World at Sentosa Pte. Ltd.
“Group”	Genting Singapore Limited, Resorts World at Sentosa Pte. Ltd., Genting Integrated Resort Operations Management Pte. Ltd. and any other company that may come under the management oversight of Genting Singapore Limited presently and/or in the future, including all their subsidiaries, affiliates and overseas offices, collectively referred to as the “Group”.
IT systems	All the facilities and functions of a computer system - distributed or workstation, and all processing environments - networked, centralised or distributed and include hardware, software, communications, networks and information/ data.
Mobile devices	All RWS issued mobile devices.
Team Members	Team Members (TM) are staff on RWS payroll.
Non-Team Members	Non-Team Members are staff not on RWS payroll.
Users	They are Team Members & Non-Team Members
HOD	Head of Department

5. POLICY

5.1. Acceptable Use

- 5.1.1. Users shall use the Group's IT systems for business purposes only.
- 5.1.2. Users shall not allow any personnel not belonging to the Group (inclusive of guests and family members) to use any of the Group's IT systems or assets (e.g. PCs/Notebooks, thumb drives, portable hard disk and mobile devices).
- 5.1.3. Users shall not disclose any sensitive or confidential information.
- 5.1.4. Users shall not access data or applications that he/she is not authorised to access.
- 5.1.5. Users shall not attempt to exploit or probe for security loopholes on the Group's IT systems or other organisations' network.
- 5.1.6. Users shall not attempt to circumvent data protection schemes and shall report any security loopholes to IT Service Desk / IT Security.
- 5.1.7. Users shall not attempt to launch denial of service attacks or perform any activity that would degrade the performance of the Group's IT systems.
- 5.1.8. Users shall not attempt to introduce any malware (e.g. computer viruses, worms and Trojan horses) to the Group's IT network.
- 5.1.9. Users shall not assist anyone to cause damage to the Group's IT systems.
- 5.1.10. Users shall not use the Group's IT systems to carry out any unlawful or illegal activities (e.g. unauthorised access to computer systems or network accounts and acts of sexual harassment) and their actions are subject to the relevant legislation and applicable laws.
- 5.1.11. Users shall complete an annual IT Security awareness training to reinforce their cybersecurity knowledge and annual acknowledgement of IT End User Policy. Failing which, IT Department may revoke user access to IT systems without user consent.
- 5.1.12. Users shall adhere to the following data governance policies:
 - i. Data Management Policy
 - ii. Data Security and Classification Policy
 - iii. Data Incident Reporting Policy

5.2. Account and Password Management

- 5.2.1. Account sharing is strictly prohibited.
- 5.2.2. Every user is assigned a unique user id and he/she is accountable for his/her account.
- 5.2.3. Password shall meet the following password complexity requirements:
 - i. At least 8 characters
 - ii. Contain characters from three of the following four categories
 - Upper case characters (A-Z)
 - Lower case characters (a-z)
 - Numeric characters (0-9)
 - Symbols (e.g. #, %, &, @)
- 5.2.4. Password shall be changed at least once every 90 days. It shall be different from the previous 5 passwords and existing password.
- 5.2.5. Password shall not be the same as user ID.
- 5.2.6. Initial or reset password shall be changed by the user upon first use.
- 5.2.7. Users shall take precautionary measures to safeguard his/her password and it shall not be disclosed to any other person.
- 5.2.8. Password retries shall be limited to a maximum of 5 attempted logons after which the user ID will be locked.

5.3. Software/Hardware

- 5.3.1. Users shall not install unauthorised or unlicensed software.
- 5.3.2. User accounts used on corporate devices shall have non-administrative user rights unless explicitly approved for use by management.
- 5.3.3. Users shall ensure that the corporate devices are connected to Group network for the virus scans and the virus signature files are updated regularly.
- 5.3.4. Users shall disconnect their IT systems from the Group network if they suspect there is a computer virus infection.
- 5.3.5. Users shall not connect any non-registered or non-corporate devices (e.g. personal notebook, USB thumb drive, external harddisk) into the Group network/system.
- 5.3.6. Users shall use Screen Lock to lock their PCs/Notebooks when they are left unattended.
- 5.3.7. Users shall shutdown and turn off their workstation before leaving office at the end of the day.
- 5.3.8. Users shall ensure that confidential information is minimally password protected and the password is transmitted separately from the protected file.
- 5.3.9. Users shall ensure the computing devices issued to them are securely stored when not in use.
- 5.3.10. In the event of theft or loss of the Group's computing devices, users shall immediately report the incident to HOD and IT Service Desk. Users shall bear the cost of replacement/repair of the Group's computing devices if the theft or damage is due to users' negligence.

5.4. Printer/Copier/Fax Machine

- 5.4.1. Users shall not leave any sensitive or confidential information unattended on the printer, copier and fax machine.
- 5.4.2. Users shall destroy any paper waste, which may contain sensitive or confidential information, using the documents shredder.

5.5. E-mail System

- 5.5.1. Users shall use the Group's e-mail system for business purposes only.
- 5.5.2. Users shall not send forged e-mail that will intimidate or harass other users, chain messages or promotional mails for profit-making purposes.
- 5.5.3. Users shall not send unsolicited e-mail using the Group-assigned e-mail address
- 5.5.4. Users shall not send messages that contain obscene, offensive or slanderous material.
- 5.5.5. Users shall not access into another user's e-mail or read someone else's e-mail without their permission.
- 5.5.6. Users shall ensure e-mail attachments and files downloaded from the Internet are scanned for viruses before execution.
- 5.5.7. Users shall not open attachments or click on URL links in e-mail from unknown or untrusted sources.
- 5.5.8. Users shall not enable any 'auto-forwarding' rules to send official e-mail to any e-mail addresses outside of the Group.
- 5.5.9. Users shall not have access to personal e-mail system from corporate devices.
- 5.5.10. Users shall notify IT Service Desk / IT Security upon receiving any suspicious or unsolicited e-mail.

RWS Restricted

5.5.11. Users shall not use Group's e-mail address for non-business purpose.

5.6. Internet Access

- 5.6.1. Users shall access the Internet for business purposes only.
- 5.6.2. User shall not have access to external storage services from corporate devices unless approved by management with business justification.
- 5.6.3. Users shall not access any web sites containing objectionable content. In addition, objectionable information, messages or postings as defined by the Singapore Laws shall not be uploaded to / downloaded from, sent or posted on the Internet respectively.
- 5.6.4. Users shall not copy programs or data protected by copyrights or by special license and any downloaded files shall be screened and verified by virus detection software before activation.
- 5.6.5. Users shall not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property rights, including the installation, distribution or used of any software that is not appropriately licensed for use by the user.
- 5.6.6. Users shall not transmit any offensive materials including but not limited to defamatory comments, personal insults, obscenity over the Internet.
- 5.6.7. Users shall not transmit the Group's information to web-based file sharing platform. Exception will only be granted for uploading of files for specific business use with Management's assessment and approval. Authorized upload of the Group's classified files on the file-sharing website shall be encrypted and zipped with password. File classification shall strictly follow the following data governance policies:
 - Data Management Policy
 - Data Security and Classification Policy
 - Data Incident Reporting Policy

5.7. Web Site, Online Forum and Web Log (Blog)

Users are prohibited to disclose the Group's proprietary information or confidential information on personal websites, social media or forums at all times. This includes, but not limited to, the Group's business decisions, products, financial information, brands and public messages.

5.8. Audit and Monitoring

- 5.8.1. The Group reserves the right to allow authorised staff to monitor Internet access, use of the Group's e-mail systems, and examine the information stored within. The Group may also conduct security checks on PCs/Notebooks assigned to the users. Data created on the Group's IT systems is deemed as the property of the Group.
- 5.8.2. Should the Group discover any users engaging in prohibited actions resulting in compromise of information security, the Group reserves the right to temporarily/permanently suspend that user's access and usage of the Group information resources.

6. DISCIPLINARY ACTIONS

Users who breach this policy may be subject to disciplinary action depending on the severity of the breach and in accordance with the Conduct Management and Disciplinary Framework.

7. IT END USER POLICY ACKNOWLEDGEMENT

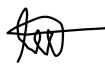
Users are to signoff to acknowledge this IT End User Policy with the form in **Annex A**.

Annex A



IT End User Policy
Acknowledgement Fo

Approval

Prepared by:	Pheng Woo TEO	Designation:	Assistant Director	Signature:	
Reviewed by:	Roger TAN	Designation:	Assistant Vice President	Signature:	
Approved by:	Alvin TAN	Designation:	Divisional President	Signature:	

Acknowledgement by IT Compliance Management Rep and above “that there are no inconsistencies between the SOP and relevant legislation”.

Acknowledged By:	NA	Designation:	NA	Signature:	NA
------------------	----	--------------	----	------------	----