CARNIVAL CORPORATION & PLC

AS-02 Acceptable Use Policy

April 2023

Purpose 3
Overview 3
Acceptable Use Policy 3
1. Compliance to Policies and Regulations 3
2. Roles and Responsibilities 4
3. Use of Technology and Business Systems 5
4. Use of Access and Credentials 5
5. Handling Information 6
6. Use of Internet Services, Email, Social Media and Apps 6
7. Monitoring and Enforcement 7
8. Consequences of Non-Compliance with this Policy 8
Appendix A – Historical Change Log 9

Purpose

This Acceptable Use Policy sets out the requirements for the use of computing and information resources by employees of Carnival Corporation and its operating companies (referred to as "Carnival" or "The Company" hereafter) wherever they are used to support the business activities of the Company.

The use of technology, and the handling and processing of confidential information, is necessary for our Company to do business. However, this introduces risks that could lead to cyber-incidents, compromise of our information assets or breaches of privacy that can have significant impacts on our Company.

The requirements of this policy are set out to manage these risks and to protect our Company, employees and guests, in line with our legal commitments and our Company values.

Overview

This policy applies to all employees of Carnival and its subsidiaries, including temporary employees and contractors / third party personal what have access to Carnival network/systems.

As a user of Carnival's information technology services and facilities, you have access to valuable Company resources, potentially confidential or sensitive information, and our company networks and business applications (collectively, "Information Assets").

Acceptable use of these Information Assets means ensuring that Company resources and technologies are used for their intended purposes while respecting the rights of others, the integrity of the physical facilities, the confidentiality of data, and the relevant license and contractual agreements.

Our values require that all employees have a duty to both follow and champion the policies and compliance requirements that relate to the use and handling of information and business systems in their care. This means being aware of the requirements that impact their work, speaking up where these requirements are not being met, and taking responsibility and ownership as needed.

To help to monitor and enforce these policies, Carnival reserves the right to monitor networks and systems in compliance with local laws, and to perform testing to monitor individual's adherence to the requirements.

If a person is found to be in violation of the Acceptable Use Policy, the Company may take disciplinary action, as described in section 8 of the document, in line with the relevant local policies and legal requirements of the operating company in question.

Acceptable Use Policy

1. Compliance to Policies and Regulations

Our policies and guidelines reflect the procedures that are in place to enable Carnival to operate within the law, and to control risks associated with misuse of information system assets.

1. It is the responsibility of all users to make themselves aware of and adhere to the Code of Conduct as they relate to the use of Technology and handling information. Where relevant, training and guidance will be provided.
2. Line managers must ensure that the processes and procedures within their area of responsibility are operated in line with appropriate policies, guidelines and regulations.

   Technical and managerial roles must make themselves aware of the published Carnival policies, standards and associated regulatory requirements that apply to the use of information systems assets as part of their work.

   These include, most notably:

   - Carnival Global Information Security Policies and Standards
   - Global Data Privacy Policy and Standards
   - Payment Card Industry Standards
   - Sarbanes Oxley IT General Controls

   Links to these resources can be found in the appendix.

3. Those responsible for interacting with suppliers or data processors that make use of our business systems or information must take reasonable steps to ensure acceptable use is followed by those third parties. This includes ensuring that contracts reflect the Carnival policies and procedures applicable to the services being provided.
4. Everyone is obliged to complete their IT information security, privacy and phishing training within 30 days of joining the company in order to access the Company's network systems and annually thereafter. This would also include all contractors and anyone else accessing our network systems on a regular basis.
5. Everyone must sign the acknowledgment of the Accessible use policy latest 5 days after getting an account in Carnival network. All permanent employees must sign once a year by mandatory eLearning module.

2. Roles and Responsibilities

The Global Chief Security Information Officer ("CISO") is responsible for communicating and ensuring awareness and compliance with this Acceptable Use Policy and supporting principles through training and education and designing and implementing the necessary procedures to ensure compliance with this policy.

The CISO has designated members of Carnival as "Information and Security Representatives" to support these activities, who may be contacted for guidance and referral to an appropriate subject matter expert.

These include:

- The Global Chief Information Security Officer (CISO) and members of the Global Information Security and Compliance Services (GISCS) team

- The Chief Privacy Officer, Data Protection Officers (DPO) and members of Data Privacy teams within the operating companies
- The Operating Company Information Technology Leaders and their respective teams
- The Human Resources Department ("HR") supports the CIO in investigating and enforcing compliance with this Acceptable Use

3. Use of Technology and Business Systems

There is a wide variety of technology in use across Carnival, ship and shore. All use of technology for Carnival business purposes must adhere to this Acceptable Use Policy.

1. Information systems may only be used for the purposes that they were intended for, and as part of legitimate business practices within Carnival. Any use that could be considered unethical or adverse to Carnival's security should be identified to a Carnival Information and Security Representative.
2. Users and administrators of technology must not misuse or abuse those systems through use of unauthorized software, or deliberate actions that may overload, destabilize or adversely affect the performance of those systems or any other.
3. All software utilized by the company must comply with agreed vendor license requirements and appropriate copyright law.
4. Those acquiring information technology services or assets on behalf of Carnival must ensure that procurement procedures are followed to ensure our suppliers meet our requirements.
5. Where permitted by brands, use of personal devices by individuals must be in line with any policies that articulate the required security controls, such as AS-04 Mobile Device Security policy and the requirements from AS-01 Data classification policy. Refer to the appendix for the list of related policies.
6. Personal devices (if in alignment with a Brand BYOD policy as mentioned in AS-04 Mobile Device Security policy), that are used by individuals to process Carnival information can be subject to investigation and enforcement action by the company in accordance with company policies and as permitted by applicable laws.
7. Use of Electronic Transferrable Media (ETM) on company assets is strictly forbidden.

4. Use of Access and Credentials

User logins and credentials are used to attribute actions made on our systems to individuals and ensure that those actions are authorized.

1. Users of systems must take due care to protect their user IDs, digital / electronic signatures, other authentication and authorization mechanisms from unauthorized use or disclosure.
2. Users must not share passwords, IDs or other authentication information (e.g., a software token) with any other individual, except where an account is known to be a legitimate account for shared use.
3. If access or authentication information to a system is disclosed in a way that may lead to a potential breach, the individual must take steps to change their passwords or authentication keys immediately and let their immediate supervisor and GISCS know as well.

4. Attempts to circumvent or override access controls, or to gain unauthorized access to Carnival systems, are not permitted unless as part of approved security testing.

5. Handling Information

The Company will handle any personal information collected by company resources in accordance with the Carnival Global Data Privacy Policy, and any operating company policies intended to meet regional requirements. Employees must be aware of these requirements and how they apply to their work.

When handling information on behalf of Carnival, users must:

1. Only access information to which they have been given authorization as part of their work, unless it has been classified by Carnival as "public" or "internal".
2. Follow any specific requirements relating to information, for example regional Data Privacy Laws and Payment Card Industry requirements, or any other relevant regulatory or contractual requirements.
3. Ensure that all electronic and hardcopy information is handled, stored and disposed of in compliance with the Data Classification Policy and Handling Guidelines, and any other applicable published policies that relate to that information. Refer to appendix for links to these policies.
4. Transmit/transport confidential information, personal information, and information assets only via mechanisms approved as being secure by a Carnival Information and Security Representative

6. Use of Internet Services, Email, Social Media and Apps

Carnival provides authorized services to its employees for the purposes of business communication, such as email, instant messaging and collaboration. Electronic and web communications are potential routes for malware infection, which has the potential to seriously damage Company resources and lead to data or privacy breaches.

Private use of company systems is forbidden. If an Operational Company decide to explicitly allow private use of company systems this needs to be agreed in a local policy under review of privacy, legal and GISCS.

All content that contravenes the Code of Business Conduct and Ethics is forbidden.

1. Services that have not been explicitly authorized by a Carnival Information and Security Representative must not be used for transmission of confidential and personal information of Carnival employees or customers, or business critical communication. If unclear if a Service is permitted, employees must formally ask GISCS for approval. Employees must not use or disclose any proprietary, confidential, or personal information that they produce or obtain during employment with the Company through any authorized services, except to the extent such use or disclosure is required by their jobs.
2. Users must not mis-use services, company provided or otherwise, in any way that conflicts with the Code of Business Conduct and Ethics.
3. All employees are required to take care to behave securely online and when using Carnival systems. This includes, but is not limited to:

- Taking care not to open any attachments or click on any links embedded in an email unless they have confidence in the identity of the sender and that it is not malicious
- Not giving away or sharing passwords or access credentials
- Not attempting to download or install software from unauthorized sources
- Seeking advice from your line manager, IT Service Desk or a Carnival Information and Security representative when confronted with potentially suspicious behavior or communications

7. Monitoring and Enforcement

Carnival operates a variety of methods to protect the business, its employees and guests from the risks that arise from use of technology and handling information, and to ensure that Acceptable Use is adhered to. This may lead to corrective action being taken, which could be improvements to processes or additional training, but could extend to formal disciplinary or legal action being taken if that is considered appropriate.

1. To help protect our company and our guests, we require all employees to speak up – report any identified or suspected security incidents immediately to your line manager, IT Service Desk or Information Security team, Carnival Information and Security representatives.
2. Carnival reserves the right to monitor user behavior and use of Information Technology and services to identify security and data protection breaches, abuse, or misuse of company systems or information. Such monitoring will be conducted in line with applicable local laws and is not intended to monitor the work performance or output of individuals.
3. Carnival may engage in activities intended to measure the understanding of good practice relating to security of the company, the privacy of personal information and company assets.
4. Monitoring activities undertaken by Carnival may or may not be communicated to our users in advance and may result in reasonable actions being taken to preserve privacy and the security and integrity of the business. Electronic communications created, sent or received using Company email systems are the property of the Company and may be accessed by a Carnival Information Security Representative or their delegate in the case of an investigation, in alignment with local laws. This includes investigations following a complaint or investigations into misconduct.
5. Electronic communications may also be subject to discovery in litigation and criminal investigations. All Carnival information held on company owned computers or devices, including emails, may be accessed as part of an investigation.
6. The Company will not disclose the content of electronic communications created, sent or received using Company resources to third parties outside of the Company unless that disclosure is required for the purposes of:
   - A company investigation
   - A law enforcement investigation
   - For other legal, investigative, audit or compliance reasons

8. Consequences of Non-Compliance with this Policy

In cases of non-compliance with this Acceptable Use Policy, the Company may initiate sanctions in line with applicable local employment laws, on a case-by-case basis. These include, but are not limited to the following:

- **Training:** For minor violations**,** Employees can be asked to participate in training regarding certain aspects of the Acceptable Use Policy, to educate and improve awareness of policy requirements in order to avoid further violations.
- **Warning:** For repeated or more significant violations, Employees can be reprimanded orally or in writing for their misconduct and asked to refrain from such behavior in the future. This consequence particularly comes into question may be appropriate if the degree of the policy violation is considered to be comparatively low.
- **Formal Warning:** Excessive or very serious violations can result in a formal warning that can be given in writing with the notification that any further cases of recurrence could lead to a termination of employment. This may be considered in addition to the above, a policy violation could have criminal or other legal consequences in cases where an employee has breached local criminal or data protection laws.

References to Policies or Standards

#	Reference (Policy/Standard)
1	AS-05 Cloud Computing Policy
2	SO-01 Event Monitoring Policy
3	AS-04 Mobile Device Security Policy
4	AS01 - Data Classification Policy
5	Data Classification Handling Guidelines
6	Carnival Global Data Privacy Policy

Appendix A – Historical Change Log

Revision, Review and Approval History

Year	Date	Name, Role	Description
2017	9/29/2017	Gary Eppinger CISO (Chief Information Security Officer)	Approved for release
2018	11/30/2018	Gary Eppinger, CISO	Approved for release
2019	11/30/2019	Gary Eppinger, CISO	Approved for release
2020	11/30/2020	Maurice Lee	Reviewed, no changes
2020	11/30/2020	Gary Eppinger, CISO	Approved for release
2021	8/12/2021	Maurice Lee	Revised version
2022	4/8/2022	Devon Bryan	Approved for release
2022	11/17/22	Sebastian Röhner	Review and revision
2022	12/26/2022	Devon Bryan	Approved for release
2023	01/17/2023	Sebastian Roehner, Director IT Governance & Compliance	Added section 3.7- “Use of Electronic Transferrable Media (ETM) on company assets is strictly forbidden.”
2023	4/28/2023	Gatha Sadhir, CISO	Approved for release