CARNIVAL CORPORATION

Acceptable Use of Technology & Information Assets Acknowledgement

Published October 2026

AIDA Carnival Costa CUNARD

Holland America Line P&O CRUISES PRINCESS SEABOURN

CONTENTS

1 Purpose & Applicability 3
2 Roles and Responsibilities....3
3 Policy 4
3.1 Cybersecurity Training & Acceptable Use Acknowledgement....4
3.2 Cyber Hygiene....5
3.3 Data & Information Handling 5
3.4 Prohibited Use 6
3.5 Suspicious Activity Reporting....7
3.6 Technology Procurement....7
3.7 Recording & Transcribing Meetings 8
3.7.1 Recording & Transcription Consent....8
3.8 Cybersecurity Monitoring 9
4 Non-Compliance 10
5 Acknowledgement 10
6 Appendix A: References....11

1 PURPOSE & APPLICABILITY

The use of technology, and the collection, processing, sharing and handling of company information, is a necessary part of doing business that inherently introduces risks to the organization that could lead to cybersecurity incidents or events that compromise the confidentiality, integrity, and availability of company networks, systems, applications, and information. Carnival Corporation and its brands, operating units, majority owned subsidiaries and controlled affiliates (collectively, the "Company") is committed to protecting the company by implementing, maintaining, and continuously improving cybersecurity policies, standards, processes and procedures that enable the Company to manage and control cybersecurity risks while adhering to applicable and local laws and regulations.

The *Acceptable Use of Technology and Information Assets Acknowledgment* outlines Company non-employee user (herein known as contractor) responsibilities and acceptable behavior, as outlined in the Global Acceptable Use of Technology and Information Assets Policy, when accessing and using company technology and when accessing, handling, processing, storing, transmitting, sharing, and disposing company data.

The Global Acceptable Use of Technology and Information Assets Policy applies to:

- Carnival Corporation and all of its affiliated brands, Corporate Units, and Operating Units (OUs).
- All Company users, including employees, vendors, contractors, third-party service providers, and consultants, accessing both internal Company IT systems (shoreside and shipboard) and third-party IT systems hosted on or off Company premises, including remote access to Company information and operational technology systems and data (herein known as "users" or "company users.").
- The access and use of information technology and operational technology including networks, systems, hardware, applications, and devices issued, owned, managed, or controlled by the Company (herein known as "technology assets").
- The creation, collection, processing, handling, transmission, sharing, and disposal of data and information owned, managed or controlled by the Company (herein known as "information assets").

The *Acceptable Use of Technology and Information Assets Acknowledgment* is intended to support the Global Acceptable Use of Technology and Information Assets Policy and company global and brand-specific privacy and workforce policies and comply with and support local privacy and workforce laws and regulations. In the instance of conflict between the Acceptable Use of Technology and Information Assets Acknowledgement and local law or executed agreements between the Company and third party, local law and executed contract requirements will apply.

2 ROLES AND RESPONSIBILITIES

All users are responsible for following and championing the security policies and standards that relate to the access, use and handling of company technology and information assets in their care. This means:

- being aware of the security requirements that impact their work
- immediately reporting suspicious activity or behavior to the Service Desk or
- speaking up where these requirements are not being met
- and taking responsibility and ownership, as needed.

All Company users are also responsible for being aware of and adhering to the:

- Global Acceptable Use of Technology and Information Assets Policy
- Code of Business Conduct and Ethics (“Code”), see Appendix B
- all other relevant policies and procedures as they relate to the use of Company technology and handling of Company information as part of fulfilling work duties.

The Global Chief Information Security Officer ("CISO") is responsible for leading Global Cybersecurity Services (GCS) in communicating and ensuring awareness with this Acceptable Use Policy through training and education, and ensuring the design and implementation of the necessary technology controls to:

- facilitate and support Global and Operating Unit cybersecurity policies and standards
- appropriately manage, treat, and report on cybersecurity risks to the organization;
- support Global and Operating Unit ethics and privacy policies and standards;
- facilitate corporate and Operating Unit compliance with cybersecurity regulatory mandates

Information Technology leads (employee users and contractor users) are responsible for ensuring their teams are building, maintaining, and administrating technology processes, systems, and controls in alignment and adherence with global cybersecurity policies and standards.

Line managers are responsible for ensuring that the systems, applications, processes, procedures and controls within their area of responsibility are operated in accordance with appropriate Company policies, guidelines and regulations. These include, most notably:

- global cybersecurity policies and standards
- global and brand data privacy policy and standards

3 POLICY

The Company has a regulatory and fiduciary obligation to ensure human users understand their roles and responsibilities in protecting the confidentiality, integrity, and availability of company systems, networks, and data collected, created, processed, transmitted, shared, stored and disposed by the Company as part of business operations.

3.1 Cybersecurity Training & Acceptable Use Acknowledgement

- Adhering to the Acceptable Use of Technology and Information Assets Policy, the global security policies and standards, and all corporate and brand policies and standards, is part of each user’s job duties and responsibilities.

- Contractor users (non-employee users) must sign the *Acceptable Use of Technology and Information Assets Acknowledgement* before being provisioned access to the Company's environment, systems, or data.
- Acknowledgment of the Acceptable Use of Technology and Information Assets Policy provides auditable evidence that individuals understand their roles and responsibilities and that the Company has fulfilled its obligations in protecting the Company's technology and information assets.

3.2 Cyber Hygiene

- Company users must take due care to secure their user IDs, company-issued individual account logins and passwords, digital / electronic signatures, and any other authentication and authorization mechanisms from unauthorized use or disclosure.
- Users must not share company-issued individual account IDs, logins or passwords, or any other authentication information (such as a software token) with anyone else.
- If access or authentication information to a system is disclosed in a way that may lead to a potential data exposure or data breach, the individual user must take steps to immediately change their individual account passwords, passwords on system/service accounts, or authentication keys and immediately report the potential security event to let their immediate supervisor, the Service Desk, and Global Cybersecurity Services.
- Users should not open any attachments or click on any links embedded in an email unless they have high confidence in the identity of the sender and that it is not malicious.
- Users must immediately report suspicious, harmful or unethical activity by:
    - Using the *Phish Alert Button (PAB)* in Outlook
    - Using the *Report this Message* function in Teams chat
    - Contacting the Service Desk (carncorp@service-now.com)
    - Contacting cyber@carnival.com.

3.3 Data & Information Handling

- Company technology and information assets may only be used for their intended purposes and as part of legitimate company business practices.
- Users must only access information to which they have been given authorization as part of their assigned roles and responsibilities, unless it has been classified by the Company as "public" or "internal".
- Users must only share, transmit, or transport confidential information (privacy or proprietary) and highly sensitive information (privacy or proprietary) via mechanisms approved as being secure by Global Cybersecurity Services. See the Global Data Classification Policy for details on the types of company data classified as per above.
- Users may only use, share or disclose company information (internal, confidential, or highly sensitive) that they produce, access, or obtain as part of fulfilling work obligations with the

company through authorized services and mechanisms, and only as required as part of fulfilling their assigned work duties. See the Global Data Classification Policy and the Global Access Management Policy.

- Users must ensure that all electronic and hard-copy information is handled, stored and disposed of in compliance with the Global Data Classification Policy and Global Data Classification and Handling Standard, and any other applicable published policies that relate to that information.
- Company data and information created, collected, accessed, processed or handled as part of fulfillment of assigned work responsibilities must only be stored in company-authorized locations.
- When and only if permitted by an Operating Unit or brand, use of personal devices to access company information or systems must be strictly limited to the usage approved by the brand, adhere to the Global Mobile Device Security Policy, Global Data Classification Policy, and any applicable brand policies. Devices not issued by the Company are considered to be Personal Devices.
- Personal devices used to access company systems and data, or engage in company related activities or communications, may be subject to investigation and legal hold, in accordance with company policies and applicable laws.

3.4 Prohibited Use

- Personal use of company systems, applications, data, or company-issued devices is strictly forbidden unless authorized by an Operating Unit or brand in compliance with local laws.
- Use of unsanctioned AI tools or free AI tools is strictly prohibited. See the Global Secure AI Standard.
- Approved Generative AI tools must only be used for the use case documented in the approved GenAI Business Productivity Enhancement (BPE) or GenAI Individual Employee Productivity (IEP) request.
- Automatic forwarding of company emails and calendar invitations to external mailboxes, email systems or web mail systems is forbidden.
- Storage of company data or information in unauthorized or personal storage locations is prohibited. Authorized storage locations can be validated with IT Help Desk.
- Use of removable storage devices including but not limited to USB flash drive, external hard drive, SD card, CD/DVD, memory card reader, mobile devices, etc. on company assets is strictly prohibited unless the storage device is a company-issued device for the sole use of fulfilling job responsibilities.
- Use of company-issued storage devices for personal use or for connection to a personal (non-company issued) device is prohibited.

- USB storage devices used as part of approved shipboard operations and maintenance activities must be scanned utilizing the onboard USB scanner prior to each connection of that USB device to any shipboard system.
- Users must not install unauthorized software or attempt to download or install software from unauthorized sources. See Global Access Management Policy.
- Installation of software or browser extensions on company-issued devices must only be done by IT.
- Use of unauthorized web applications is prohibited. Users must contact the Service Desk to determine if a web application is authorized for use.
- Connection to any cloud services is prohibited unless these services are approved by Global Cybersecurity Services and in adherence with the Global Cloud Computing Policy and/or the Global Asset Management policy.
- Users must not engage in deliberate or negligent actions that could overload, slow, destabilize, damage, break, or harm the performance of company technology, networks, systems, applications, or any other related technology components.
- Users must not misuse company systems, applications or information in any way that conflicts with the Code of Business Conduct and Ethics. Any content or activities that contradict the Code of Business Conduct and Ethics are forbidden.
- Any attempts to circumvent or override access controls, or to gain unauthorized access to Company systems or data, are not permitted unless as part of approved security testing.

3.5 Suspicious Activity Reporting

- Users must contact their line manager, the Service Desk or Global Cybersecurity Services (GCS) when confronted with potentially suspicious, unethical, or harmful behavior or communications.
- Services that have not been explicitly authorized by GCS may not be used for transmission of confidential and personal information of Company employees or customers, or business critical communications. If unclear if a service is permitted, users must contact GCS for approval.

3.6 Technology Procurement

- Users responsible for procuring or managing third party services or relationships must follow corporate and OU technology procurement procedures as defined by their Operating Unit and the Carnival Corporation Contract Authorization and Administration Policy. This includes:
    - ensuring the third party vendor completes a Third Party Security Risk Assessment upon vendor selection and as outlined in Global Third Party Security Risk Management Policy;
    - ensuring that contracts and agreements include appropriate cybersecurity language and provisions;

- ensuring the third party vendor is familiar with and adheres to all global cybersecurity policies and standards applicable to the services or goods the third party vendor is fulfilling or supplying.

3.7 Recording & Transcribing Meetings

Company users must not use any other system for meeting recordings outside of Microsoft Teams, unless approved by the Chief Financial Officer and General Counsel of the company.

- Meetings and transcripts must not to be shared with external parties.
- Meetings and transcripts are prohibited when legal counsel, internal or external, is present to preserve the confidentiality of privileged legal discussions (except where expressly requested and authorized by legal counsel).
- Recordings and transcripts subject to a legal hold or discovery request must be preserved in accordance with the Corporate Policy and Procedure for Privileged and Confidential Matters and relevant instruction provided by the Global Legal or its designee ("Authorized Counsels"). Such preservation supersedes the obligation to delete a recording or transcript within defined deletion rules and remains until explicitly released by authorized Counsels.

3.7.1 RECORDING & TRANSCRIPTION CONSENT

- Consent to record or transcribe must be gained from all meeting participants prior to recording or transcription being activated and the meeting host must confirm the meeting platform provides a written notification to all meeting participants upon activation of the recording or transcription.
- If the meeting recording or transcription is paused during a meeting break or to preserve confidentiality of a discussion, then participant consent to the recording or transcription must be restarted from all participants and the meeting host must confirm that the meeting platform has provided written notification of the recording or transcription to the meeting participants.
- Meetings hosted by external parties should not be recorded or transcribed unless there is an agreement/contract in place that outlines confidentiality requirements from that party.
- Explicit consent to the recording or transcription must be obtained from all participants of meetings with nine (9) or less participants.
- A prior notification that a recording or transcription of the meeting must be posted to all attendees for meetings with ten (10) individuals or more, including internal company training videos or recordings, and town hall-style meetings, and whether the participation is in-person and/or virtual.
- Continued presence by an individual in the meeting without an objection being raised in response to the meeting recording or transcription notification, is considered as implicit consent from the individual.

3.8 Cybersecurity Monitoring

The Company has a regulatory obligation and responsibility under *Security by Design* and *Privacy by Design* principles within the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Sarbanes-Oxley (SOX) and Payment Card Industry Data Security Standard (PCI-DSS), among other regulations and laws to which the Company is subject, to:

- monitor and alert on company networks, systems and data for suspicious and potentially malicious activity and immediately respond to and investigate, control, contain, and eradicate any actor(s) (person and non-persons accounts) to minimize the risk to the confidentiality, integrity, and availability.
- monitor and alert on user account behavior (person and non-person / service accounts controlled by the Company) and use of company technology and company information by those accounts for indicators of unauthorized or unusual behavior and indicators of compromise, abuse, or misuse of company systems or information, and potential security events or incidents that could result in data exposure, data loss, or system breach.
- Monitor the perimeter of the Company's environments, the user account (person and non-person / service account) activity, and the threat landscape within which the Company operates.

Such cybersecurity monitoring will be conducted in line with applicable local laws and does not monitor the work performance or output of individuals.

- Monitoring activities undertaken by the Company may or may not be communicated to company users in advance and may result in reasonable actions being taken to preserve privacy and the security and integrity of the business.
- The Company is legally accountable and responsible for all electronic communications created, sent, or received on company email or messaging systems. As such, electronic communications created sent, or received on company email or messaging systems may be placed on legal hold and/or accessed by:
    - GCS Security Operations;
    - Executive corporate and brand Leadership including the CISO;
    - HR Leadership;
    - Corporate and brand privacy officers (DPOs);
    - corporate and brand, internal and external Legal Counsel;
    - Operating Unit / brand local regulatory bodies or counsels;
    - or delegates of the above in the case of an investigation, in alignment with local laws. This includes investigations following a complaint, investigations of a cybersecurity event or incident, or investigations into misconduct.
- Electronic communications may be subject to discovery in litigation and criminal investigations. All company information held on company-owned computers or devices, including emails, may be accessed as part of an investigation.

- The company will not disclose the content of electronic communications created, sent or received using company resources and assets 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.

4 NON-COMPLIANCE

Third Party supplied resource users (non-employee users / contractors) found to be non-adherent with global cybersecurity policies or standards will be reported to the third party / vendor for handling and actioning according to the executed agreements.

5 ACKNOWLEDGEMENT

As part of your work duties, it is essential that you know and understand your responsibilities in protecting the confidentiality, integrity, and availability of company technology and information resources for which the Company (Carnival Corporation and its brands, operating units, majority owned subsidiaries and controlled affiliates) manages, controls, and is accountable. The *Acceptable Use of Technology and Information Assets Acknowledgement* details how company technology and information resources must be, and must not be, accessed, used, and reported on (standards), by company non-employee users (contractors), as per the Global Acceptable Use of Technology and Information Assets Policy, and to support business activities and minimize security risks to the Company and its users, including employees, vendors, contractors, third-party service providers, and consultants.

By acknowledging the *Acceptable Use of Technology and Information Assets* you are indicating that you have received, read, understand, and intend to apply and adhere to these standards as part of your work duties and responsibilities. Acknowledgement does not represent your consent to the monitoring of your performance, access to your communications without documented, necessary purpose, or a waiver of your rights under applicable law.

Company Name

_____

User Full Name

_____

Signature

_____

Signature Date

_____

6 APPENDIX A: REFERENCES

Note: All below policies and standards are accessible via the Company's intranet. Contact cybergovernance@carnival.com if unable to access the Company's intranet.

- Code of Business Conduct and Ethics
- Corporate Policy and Procedure for Privileged and Confidential Matters
- Global Acceptable Use of Technology and Information Assets Policy
- Global Third Party / Supply Chain Cybersecurity Risk Management Policy
- Global Cloud Computing Policy
- Global Event Monitoring Policy
- Global Mobile Device Security Policy
- Global Data Classification Policy
- Global Data Classification and Handling Standard
- Global Technology Asset Management Policy
- Global Secure AI Standard