

SECTION Information Technology	NUMBER AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT Acceptable Use		PAGE Page 1 of 16

### I. Purpose

The purpose of the Indian River County Acceptable Use Policy is to establish acceptable practices regarding the use of Indian River County information technology resources in order to protect the confidentiality, integrity and availability of information created, collected, and maintained.

### II. Scope

This policy applies to all personnel which are defined as staff, contractors, and consultants that are employed or contracted with the divisions of the Indian River Board of County Commissioners, including its officers, departments, and special dependent districts. This includes the information technology governance of system operations for all departments and divisions, including but not limited to Human Resources, Budget, Information Technology, Community Development, Parks and Recreation, Emergency Services, Public Works, Utility Services, County Attorney's Office, the Emergency Services District, the Solid Waste Disposal District and General Services.

#### III. Definitions

Information Technology Resources - Information Technology Resources include any electronic equipment, hardware, software or services that are assigned and available for employees to use in the course of their employment. These resources include, but are not limited to, the following: computer workstations and servers, laptops, printers, copy machines, scanners, cellular phones, tablets, fax machines, software applications, Internet access, voice mail and email

Site Moderator - Site Moderators are the individuals responsible for managing and maintaining the commenting community for a given social media site or blog.

### IV. Policy

#### 1. Acceptable Use

a. Personnel are responsible for complying with County policies when using County information technology resources. If requirements or responsibilities are unclear, please seek assistance from the Information Technology Department.



SECTION	NUMBER	EFFECTIVE DATE
Information	AM-1200-21	01/31/2023
Technology		
SUBJECT		PAGE
Acceptable Use		Page 2 of 16

- b. Personnel must promptly report harmful events or policy violations involving County information technology resources or information to their manager or a member of the Incident Response Team (CIRT@indianriver.gov). Events include, but are not limited to, the following:
  - i. <u>Technology incident:</u> any potentially harmful event that may cause a failure, interruption, or loss in availability to County information technology resources.
  - ii. <u>Data incident:</u> any potential loss, theft, or compromise of County information.
  - iii. <u>Unauthorized access incident:</u> any potential unauthorized access to a County information technology resource.
  - iv. <u>Facility security incident:</u> any damage or potentially unauthorized access to a County owned, leased, or managed facility.
  - v. <u>Policy violation:</u> any potential violation to this or other County policies, standards, or procedures.
- c. Personnel shall not purposely engage in activities that may:
  - i. harass, threaten, impersonate, or abuse others;
  - ii. degrade the performance of County information technology resources;
  - iii. deprive authorized County personnel access to a County information technology resource;
  - iv. obtain additional information technology resources beyond those which have been allocated;
  - v. circumvent County computer security measures.
- d. Personnel shall not download, install, or run applications or utilities that reveal or exploit weakness in the security of a County information technology resource. For example, County personnel shall not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any County information technology resource.



SECTION Information Technology	<b>NUMBER</b> AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT Acceptable Use		PAGE Page 3 of 16

- e. Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using County information technology resources. Software products that are not appropriately licensed for use by the County shall not be installed on County information technology resources.
- f. All work products, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, created or developed using County information technology resources are the property of County.
- g. Use of encryption shall be managed in a manner that allows designated County personnel to promptly access all data.
- h. County Information technology resources are provided to facilitate County business and shall not be used for personal financial gain.
- i. Personnel are expected to cooperate with incident investigations, including any federal or state investigations.
- j. Personnel should not intentionally access, create, store or transmit material which County may deem to be offensive, indecent, or obscene.

#### 2. Access Management

- a. Access to County information technology resources and information is based on the principle of least privilege, which limits users' access rights to only what is strictly required to perform their job functions.
- b. Personnel are permitted to use only those information technology resources issued to them by the County's Information Technology Department and shall not attempt to access any data or application programs contained within County information technology resources for which they do not have authorization or explicit consent.
- c. All remote access connections made to internal County networks and/or environments must be made through approved, and County-provided, virtual private networks (VPNs).
- d. Personnel shall not divulge any information technology resource identity and access management information to anyone not specifically authorized to receive such information, including Information Technology support personnel.
- e. Personnel must not share their identity and access management information, including:
  - i. Account passwords,



SECTION Information Technology	<b>NUMBER</b> AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT Acceptable Use		PAGE Page 4 of 16

- ii. Personal Identification Numbers (PINs),
- iii. Security Tokens (i.e. Smartcard),
- iv. Multi-factor authentication information
- v. Access cards and/or keys,
- vi. Digital certificates,
- vii. Similar information or devices used for identification and authentication purposes.
- f. Access cards and/or keys that are no longer required must be returned to a supervisor or the Human Resources Department.
- g. Lost or stolen access cards, security tokens, and/or keys must be reported to a supervisor **and** the Information Technology Department as soon as possible.

#### 3. Authentication/Passwords

- a. All personnel are required to maintain the confidentiality of identity and access management information.
- b. If authorized by the Information Technology Department, any group/shared identity and access management information must be maintained solely among the authorized members of the group.
- c. All passwords, including initial and/or temporary passwords, must be constructed, and implemented according to the following County rules (AM 1200-6):
  - i. Must meet all requirements including minimum length, complexity, and reuse history.
  - ii. Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
  - iii. Must not be the same passwords used for non-business purposes.
- d. Unique passwords should be used for each system, whenever possible.
- e. User account passwords must not be divulged to anyone.
  - i. County support personnel and/or contractors should never ask for user account passwords.
- f. If the security of a password is in doubt, the password shall be changed immediately.



SECTION	<b>NUMBER</b> AM-1200-21	EFFECTIVE DATE
Information		01/31/2023
Technology		
SUBJECT		PAGE
Acceptable Use		Page 5 of 16

- g. Personnel shall not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software.
- h. Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with County, if issued.

#### 4. Clear Desk/Clear Screen

- a. Personnel shall log off from applications or network services when they are no longer needed. At a minimum, personnel shall log off at the end of each business day.
  - i. Workstations shall be left in a power on state so that administration tasks may be performed on the workstation.
- b. Personnel shall log off or lock their workstations and laptops when their workspace is unattended.
- c. Confidential or internal information shall be removed or placed in a locked drawer or file cabinet when the workstation is unattended and at the end of the workday if physical access to the workspace cannot be secured by other means.
- d. File cabinets containing confidential information shall be locked when not in use or when unattended.
- e. Physical and/or electronic keys used to access confidential information shall not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- f. Laptops shall not be left unattended when in use away from the office. Laptops shall remain in possession of the person that they are issued to or stored in a locked drawer or cabinet when not in use (e.g. end of the workday).
- g. Passwords must not be stored on or under a computer or in any other physically accessible location.
- h. Copies of documents containing confidential information should be immediately removed from printers and fax machines.

#### 5. Data Security

a. Personnel shall use approved encrypted communication methods when sending confidential information over public computer networks (Internet).



SECTION Information Technology	<b>NUMBER</b> AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT		PAGE
Acceptable Use		Page 6 of 16

- b. Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
- c. Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity and consistent with Public Records Law and retention requirements.
- d. All electronic media containing confidential information must be disposed of securely and consistent with Public Records Law and retention requirements. Please contact the Information Technology Department for guidance or assistance.

#### 6. Email and Electronic Communication

- a. Auto-forwarding electronic messages outside the County internal systems is prohibited.
- b. Electronic communications shall not misrepresent the originator or County.
- c. Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
- d. Accounts must not be shared without prior authorization from the Information Technology Department, with the exception of calendars and related calendaring functions.
- e. Personnel shall not use personal email accounts to send or receive County information.
- f. Any personal use of County provided email shall not:
  - i. Involve solicitation.
  - ii. Be associated with any religious or political cause or entity.
  - iii. Have the potential to harm the reputation of County.
  - iv. Forward chain emails.
  - v. Contain or promote threatening or unethical behavior.
  - vi. Violate local, state, federal, or international laws or regulations.
  - vii. Result in unauthorized disclosure of County information.
  - viii. Or otherwise violate any other County policies.
- g. Personnel shall send confidential information using only County approved secure electronic messaging solutions.
- h. Personnel must use caution when responding to, clicking on links within, or opening attachments included in electronic communications.



ADMINISTRATIVE	
<b>POLICY MANUAL</b>	

<b>NUMBER</b> AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
	PAGE Page 7 of 16

- Personnel should use discretion in disclosing confidential or internal information in Out
  of Office or other automated responses, such as employment data, internal telephone
  numbers, location information or other sensitive data.
- j. Personnel email signatures shall be limited to only the following items:
  - i. Name
  - ii. Professional Designations or Certifications
  - iii. Job Title
  - iv. Department
  - v. County Work Location Address
  - vi. Office Phone Number
  - vii. Mobile Phone Number
  - viii. County issued email address
  - ix. County approved logos
  - x. County approved public records declaration or statement
- k. Electronic mail (e-mail) messages made or received by County employees in connection with the transaction of official business are public records.

#### 7. Hardware and Software

- a. All information technology hardware must be formally approved by the Information Technology Department before being connected to County networks.
- Software installed on County information technology resources must be approved by the Information Technology Department and installed by County Information Technology personnel.
- c. All County information technology resources taken off-site must be physically secured at all times.
- d. Personnel shall not allow family members or other non-employees to access County information technology resources.

#### 8. Internet

a. The Internet must not be used to communicate County confidential or internal information, unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established. Only County approved electronic distribution methods may be used for this purpose.



SECTION Information Technology	<b>NUMBER</b> AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT		PAGE
Acceptable Use		Page 8 of 16

- b. Use of the Internet with County networking or computing resources must only be used for business-related activities. Unapproved activities include, but are not limited to:
  - i. Recreational games
  - ii. Streaming media
  - iii. Personal social media
  - iv. Accessing or distributing pornographic or sexually oriented materials
  - v. Attempting or making unauthorized entry to any network or computer accessible from the Internet
  - vi. Any activity that would violate any other County policy
- c. Access to the Internet from outside the County network using a County owned computer must adhere to all of the same policies that apply to use from within County facilities.

#### 9. Mobile Devices

- a. County does not allow personally owned mobile devices to connect to the County enterprise internal network.
- b. Mobile devices that access County email servers must have a PIN or other authentication mechanism enabled.
- c. Confidential information should only be stored on devices that are encrypted in compliance with the County Encryption Standard.
- d. County confidential information should not be stored on any personally owned mobile device.
- e. Theft or loss of any mobile device that has been used to create, store, or access confidential or internal information must be reported to the County Information Technology Department immediately.
- f. All mobile devices must maintain up-to-date versions of all software and applications.
- g. All personnel are expected to use mobile devices in an ethical manner.



SECTION Information Technology	NUMBER AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT		PAGE
Acceptable Use		Page 9 of 16

- h. In the event that there is a suspected incident or breach associated with a mobile device, it may be necessary to remove the device from the employee's possession as part of a formal investigation.
- i. All mobile device usage in relation to County information technology resources may be monitored, at the discretion of County.
- j. County Information Technology support for personally owned mobile devices is limited to assistance in complying with this policy.
  - i. County Information Technology support may not assist in troubleshooting device usability issues.
- k. Texting or emailing while driving is not permitted while working or using County vehicles. Only hands-free talking while driving is permitted when using County resources.

#### 10. Physical Security

- a. Personnel must badge in and out of access-controlled areas. Piggy-backing, tailgating, door propping and any other activity to circumvent door access controls are prohibited.
- b. Visitors accessing card-controlled areas of facilities must be accompanied by authorized personnel at all times.
- c. Eating or drinking are not allowed in data centers.
- d. Caution must be used when eating or drinking near workstations or information processing facilities.

#### 11. Privacy

a. Information created, sent, received, or stored on County information technology resources are not private and may be accessed by County Information Technology employees at any time, under the direction of County executive management and/or Human Resources, without knowledge of the user or resource owner.



SECTION Information Technology	<b>NUMBER</b> AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT Acceptable Use		PAGE Page 10 of 16

- b. The County may log, review, and otherwise utilize any information stored on or passing through its information technology resources.
- c. Systems Administrators, County Information Technology staff, and other authorized County personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges shall not access files and/or other information that is not specifically required to carry out an employment-related task.

#### 12. Removable Media

- a. The use of removable media for storage of County information must be supported by a reasonable business case.
- b. All removable media use must be approved by the County Information Technology Department prior to use.
- c. Personally owned removable media use is not permitted for storage of County information and shall not be interfaced with County information technology resources.
- d. Personnel are not permitted to connect removable media from an unknown origin without prior approval from the County Information Technology Department.
- e. Confidential and internal County information should not be stored on removable media without the use of encryption.
- f. All removable media must be stored in a safe and secure environment.
- g. The loss or theft of a removable media device that may have contained any County information must be reported to the County Information Technology Department immediately.

#### 13. Security Training and Awareness

a. All new personnel must complete an approved cybersecurity awareness training prior to, or within 10 business days of, being granted access to any County Information technology resources.



SECTION Information Technology	<b>NUMBER</b> AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT Acceptable Use		PAGE Page 11 of 16

- b. All personnel must be provided with and acknowledge they have received and agree to adhere to the County Information Security Policies before they are granted access to County Information technology resources.
- c. All personnel must complete the annual security awareness training.

#### 14. Social Media

- a. Communications made with respect to social media shall be made in compliance with all applicable County policies.
- b. Personnel are personally responsible for the content they publish online.
- c. Creating any public social media account intended to represent County, including accounts that could reasonably be assumed to be an official County account, requires the permission of the County Administrator.
- d. When discussing the County or County related matters, you must:
  - i. Identify yourself by name,
  - ii. Identify yourself as a County representative, and
  - iii. Make it clear that you are speaking for yourself and not on behalf of the County, unless you have been explicitly approved to do so.
- e. Personnel shall not misrepresent their role at County.
- f. When publishing County-relevant content online in a personal capacity, a disclaimer must accompany the content.
  - i. Example disclaimer; "The opinions and content are my own and do not necessarily represent County's position or opinion."
- g. Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).
- h. Discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with County will not be tolerated.



SECTION Information Technology	<b>NUMBER</b> AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT		PAGE
Acceptable Use		Page 12 of 16

- Confidential information, internal communications and non-public financial or operational information may not be published online in any form.
- j. Personal information belonging to County residents may not be published online.
- k. Personnel approved to post, review, or approve content on County social media sites must adhere to the following County Social Media Management Procedures.
  - i. This Social Media Management Procedure provides guidelines and requirements for posting Indian River County business related content on non-County owned Internet sites. These sites are governed by the Terms and Conditions along with the Privacy Policy as defined on each site. It is the responsibility of each Department Director, whose department has a social media site, to ensure staff adheres to the Terms and Conditions of the social media sites. Social media sites must be approved by the County Information Technology Department and the County Administrator. Facebook, Twitter, YouTube, Instagram, and Nextdoor are approved sites.
  - ii. The Director of the department requesting the account must request County Administrator approval, in writing, for the creation of accounts for posting County content on non-County owned social media sites. The County Information Technology Department is responsible for account creation and maintaining passwords and login information for each site. Primary social media sites for Indian River County will be maintained by the County Information Technology Department.
  - iii. The name of a site will include Indian River County and the Division or Program name. Only official department/division logos are to be used on the site.
  - iv. The Director of the department or division creating the account will be responsible for approving staff members that are authorized to maintain the site.
  - v. The Director of the department or division posting any County content will be responsible for assuring all information is current, accurate, and appropriate for dissemination to the public. In all cases, postings must be professional, courteous, and pertain specifically to official County business and promotion of County programs or events.



SECTION Information Technology	NUMBER AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT Acceptable Use		PAGE Page 13 of 16

- vi. The purpose of these sites is to distribute information to the public. Staff will not reply to comments posted by site visitors, unless the County Administrator approves a compelling reason for two-way communication. Staff may answer questions asked in post comments using the private chat feature of the social media site.
- vii. Launching a site creates a responsibility for the registering department to be active in the maintenance of the site. Responsibilities of the site moderator include:
  - 1. Posting fresh material in a timely fashion to keep site subscribers interested and engaged.
  - 2. Responding to comments in a timely manner if two-way communication is enabled.
  - 3. Deleting sites that are dormant.
- viii. As with all communications, all public records requirements and laws apply to these sites. As the County does not own or operate these sites, information posted or received must be maintained in electronic format by the County Information Technology Department and shall be available to print upon public records request, for the applicable retention period, in order to fulfill public information requests should the site go down or be abolished.
- ix. Indian River County reserves the right to remove or hide inappropriate content, including, but not limited to:
  - 1. Profane language or content;
  - 2. Personal attacks;
  - 3. Sexual content or links to sexual content;
  - 4. Content that includes unlawful conduct;
  - 5. Comments that are clearly off topic from the posted topics;
  - 6. Advertising services, entities, products or solicitations of commerce;
  - 7. Spam or links to other websites, pages, or accounts;
  - 8. Information that may compromise the safety or security of the public or public systems;
  - 9. Content that defames any person, group, or organization.



SECTION Information Technology	<b>NUMBER</b> AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT		PAGE
Acceptable Use		Page 14 of 16

#### 15. Voicemail

- a. Personnel should use discretion in disclosing confidential or internal information in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive data.
- b. Personnel shall not access another user's voicemail account unless it has been explicitly authorized.
- c. Personnel must not disclose confidential information in voicemail messages.

#### 16. Incidental Use

- a. As a convenience to County personnel, incidental use of information technology resources is permitted. The following restrictions apply:
  - Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, and so on, is restricted to County approved personnel; it does not extend to family members or other acquaintances.
  - ii. Incidental use should not result in direct costs to County.
  - iii. Incidental use should not interfere with the normal performance of an employee's work duties.
  - iv. No files or documents may be sent or received that may cause legal action against, or embarrassment to, the County or its residents.
- b. Storage of personal email messages, voice messages, files and documents within County Information technology resources must be kept to a minimum.
- All information located on County information technology resources is owned by County
  may be subject to public records requests and may be accessed in accordance with this
  policy.

### V. Disciplinary Action

All employees found to have violated any of the policy statements defined within this policy will be subject to discipline up to and including dismissal in accordance with County policy.



SECTION
Information
Technology
SUBJECT

Acceptable Use

**NUMBER** AM-1200-21 **EFFECTIVE DATE** 01/31/2023

PAGE

Page 15 of 16

### VI. Procedures, Guidelines, Forms and Other Related Resources

#### VII. References

APM 1200-3 Awareness and Training

APM 1200-5 Planning

APM 1200-6 Identification and Authentication

APM 1200-7 System and Communication Protection

APM 1200-9 Access Control

APM 1200-11 Assessment, Authorization, and Monitoring

APM 1200-14 Media Protection

APM 1200-15 Physical and Environmental Protection

APM 1200-16 Personnel Security

APM 1200-20 Personally Identifiable Information Processing and Transparency

### VII. Responsibility

Information Technology Department

### VIII. Authority Approval and Signature

Approved:	
Michael Zito	 
Interim County Administrator	



SECTION Information Technology	<b>NUMBER</b> AM-1200-21	<b>EFFECTIVE DATE</b> 01/31/2023
SUBJECT		PAGE
Acceptable Use		Page 16 of 16

### VIII. History

VERSION	DATE	CHANGES	DEPT/INDIVIDUAL
1.0	01.01.23	Initial Publication	IT/D. Russell