IT - General Employee Policies

Last Updated September 2021

This document contains IT policies and policy excerpts applicable to general Racine County employees and contractors.

Scope

These policies apply to and must be complied with by all Racine County Users.

The User agrees to abide by these policies while employed or contracted with Racine County.

Roles and responsibilities of each function pertaining to the protection of Racine County owned systems and data are documented in Racine County Policy Management Policy.

The User is responsible for understanding the terms and conditions of these policies. Exemptions to this policy shall follow the process defined in Racine County Policy Management Policy.

These policies are subject to change.

These policies apply to any IT systems owned or leased by Racine County. They also apply to any computing device or physical information (paperwork including but not limited to documents and files) regardless of ownership, which either contains Racine County-owned data or that, if lost, stolen, or compromised, and based on its privileged access, could lead to unauthorized data or information disclosure.

Disciplinary Action

Management reserves the right to revoke access at any time for violations of these policies and for conduct that disrupts the normal operation of Racine County information systems or violates federal, state, or local law.

Any User who has violated these policies may be subject to disciplinary action, up to and including termination of employment or contract with Racine County.

Racine County will cooperate with appropriate law enforcement if any User may have violated federal, state, or local law.

Document Change Management

All changes to this document shall follow the process defined in Racine County Policy Management Policy.

ACCEPTABLE USE

General

Use of Racine County's IT systems is provided to assist in the fulfillment of job duties. Racine County information and IT systems shall be used in an approved, ethical, and lawful manner to avoid loss or damage to Racine County's operations, image, or financial interests and to comply with official acceptable use policies and procedures. Users shall contact the IT Department prior to engaging in any activities not explicitly covered by these policies. Prohibited use includes:

- Violating any local, state, or federal laws, including those involving fraud, defamation, slander, or misrepresentation.
- Sending, receiving, or printing copyrighted materials, including articles and software, in violation of copyright laws.
- Sending, receiving, printing, or capturing proprietary business data, trade secrets, or other confidential information in violation of company policy or proprietary agreements.
- Using offensive, harassing, or threatening statements or language, including disparagement of others based on their race, culture, national origin, gender/gender identification, sexual orientation, age, disability, or religious or political beliefs.
- Creating a hostile or intimidating work environment.
- Sending or soliciting sexually oriented messages or obscene images.
- Operating a business, usurping business opportunities, sending SPAM email or soliciting money for personal gain.
- Gambling or engaging in any other activity in violation of local, state, or federal law.
- Attempting to obtain inappropriate or authorized access to data or systems
- Sending viruses or malware or attempting to cause denial of service (DOS) attacks against others.
- Impersonating others, whether inside or outside the organization.

Mobile Devices

Mobile Devices and Bring Your Own Device (BYOD) use are provided by the organization to assist in the fulfillment of job duties.

Requirements for Safe Device Use

- Do not share devices with other employees or non-Racine County personnel.
- Always secure devices with passwords/PINs/biometric mechanisms. Do not attempt to circumvent or disable these mechanisms.
- Avoid using public or unsecured network connections while using mobile devices for work.
- Operating system and application patches should be installed within 30 days of release.
- Mobile devices shall have active and up-to-date anti-malware/virus protection software and confirm that all critical and security patches/operating system updates are installed on mobile devices on a periodic basis. Do not attempt to disable to bypass anti-malware software nor prevent or delay the installation of patches/operating system updates.
- Label mobile devices with your contact information so they can be returned if lost.
- Turn off Bluetooth and other unnecessary services.
- Staff are responsible for ensuring all important files stored on the mobile device are backed up on a regular basis.
- Mobile devices generally lack a cursor to hover over potentially suspicious links to reveal the true website address (a common way to spot phishing attempts); refrain from accessing such links on a mobile device; wait to use a laptop or desktop machine to analyze the website address.
- No personal identifier data such as social security numbers, driver's license numbers or bank/credit card numbers are to be kept on mobile devices.
- Be cognizant of your surroundings and keep an eye out for strangers who may attempt to view or overhear confidential details being shared or discussed.
- Notify your manager as well as the IT department immediately if the device is lost or stolen.

Bring Your Own Device (BYOD)

Use Requirements and Conduct policies apply equally to BYOD equipment as they do to organization owned equipment.

- Use of personal equipment is subject to the device lifecycle policy. Hardware or software unsupported by the manufacturer or vendor is considered insecure and is forbidden for use. The organization may at any time disallow the use of personal equipment deemed incapable of connecting securely or that isn't interoperable with software needed for the employee to fulfill their duties.
- Use of personal equipment may require the installation of qualified security software, such as anti-virus or anti-malware software. Licenses for this software will be provided by the organization, and definition/software updates must be performed on a regular and timely basis by the employee.

- Employees separating from the organization must confirm with IT that BYOD equipment used to access data belonging to the organization has been cleared of all such data.
- If using BYOD, consult the manufacturer/vendor/carrier for support of your device before requesting assistance from the company IT department if the issue is related to the device.
- Employees must consent to device management by Racine County through Microsoft and other applications.

Virtual Private Network (VPN) Usage

Certain Racine County information systems contain highly restricted information and may be accessible only via the County's network. When authorized individuals have a need to reach these restricted resources remotely, they may be provided with access to a Racine County VPN solution (Netmotion, Cisco AnyConnect, or Palo Alto Global Protect) which provides a mechanism for secure access.

- All other standards of this Acceptable Use policy extend to resources accessed via the VPN.
- Use a password-protected profile on the computer to prevent unauthorized individuals (e.g., family members, friends) from accessing information.
- Not allow any unauthorized users to access Racine County resources via the VPN.
- Disconnect from the VPN when it is no longer needed.

Internet Usage

Internet use is provided by the organization to assist in the fulfillment of job duties. Occasional and reasonable personal use of the organization-provided internet connection is permitted if it does not interfere with work performance or the security of IT systems. Employees should not expect any degree of privacy when accessing the internet via organization-owned systems. Internet use on organization-owned devices, personal devices permitted under BYOD policy, and/or organization-owned or subsidized internet connections are subject to monitoring or review.

Employee internet usage should be consistent with the same standards of professional conduct expected offline. Under no circumstances should the organization's resources be used for purposes that are in violation of applicable state or federal laws, or to access or transmit sexually explicit content or other material incorporating vulgar, sexist, racist, threatening, violent, or defamatory language, nor to retrieve or disseminate internal information without prior authorization.

Racine County may remove, block, filter or restrict by any other means any materials that, in our sole discretion, may be illegal, may subject Racine County to liability, may

violate this policy and/or fall within our prohibited categories (crypto-mining, drugs, alcohol, auctions, copyright-infringement, dating, extremism, gambling, games, hacking, hunting, adult, phishing, anonymizers, streaming-media, weapons, web-advertisements).

Requirements for Safe Browsing

- Avoid questionable websites or those of a prohibited category.
- Always ensure Sophos Security services are working and enabled.
- Use a modern, supported, and up-to-date browser.
- Browsers will proactively warn users before accessing websites with expired security certificates or that are known to host malware.
- Inform IT if a previously used website displays errors related to expired or revoked certificates or malware.

Prohibited

- Browsing explicit pornographic or hate-based web sites, hacker or cracker sites, or other sites that Racine County has determined to be off-limits.
- Posting, sending, or acquiring sexually explicit or sexually oriented material, hate based material, hacker-related material, or other material determined to be off-limits.
- Posting or sending sensitive information outside of Racine County without management authorization.
- Using other services available on the Internet, such as FTP or Telnet, on systems for which the user does not have an account, or on systems that have no guest or anonymous account for the service being used.
- Posting commercial announcements or advertising material.
- Promoting or maintaining a personal or private business.
- Receiving news feeds and push data updates unless the material is required for Racine County business.
- Using non-work-related applications or software that occupy excess workstation or network processing time (e.g., processing in conjunction with screen savers).
- Bypassing restrictions on websites.
- Installing plug-ins or extensions without prior written authorization from IT.

Social Media

- Access to social networking services (Facebook, LinkedIn, Twitter, Instagram, Medium, company blogs, press releases, etc.) for organization purposes shall be provided only to authorized personnel.

- As with personal internet access, personal use of social media and instant messaging is acceptable as long as it involves professional conduct and appropriate content, and it doesn't impede an employee's ability to perform their work or jeopardize the security of IT systems.
- Employees should never post, refer/allude to, tag, or disclose company activities on social media without prior authorization from their manager and/or Human Resources, as appropriate.

Media Streaming Services

- Use of Racine County-owned systems or subsidized internet connections for media streaming services (Netflix, YouTube, etc.) is limited to circumstances necessary for fulfilling job responsibilities.
- Video streaming can consume significant network bandwidth, causing delayed access to and/or preventing other users from accessing legitimate business resources and completing business-critical tasks.

Internet of Things (IoT)

- Use of IoT devices, including but not limited to smart speakers, fitness wearables, environmental monitors, and motion sensors, is subject to prior written approval by the IT department.
- Restrictions for BYOD and confidential/copyrighted material applies to user-owned IoT devices.
- IoT devices that contain company data must be stored securely and not provided to unauthorized personnel.

Software Installations

If you want to install software on Racine County devices, you must contact the IT department and request to have the software installed. Users are prohibited from installing any software on any Racine County technical resource without the express prior written permission from the IT department.

Involving the IT department ensures that Racine County can manage the software on our systems, prevent the introduction of computer viruses, and meet our obligations under any applicable software licenses and copyright laws. Computer software is protected from unauthorized copying and use by federal and state law; unauthorized copying or use of computer software exposes Racine County and the individual user to substantial fines and exposes the individual to imprisonment. Therefore, users may not load personal software onto Racine County's systems and may not copy software from Racine County for personal use.

Racine County will cooperate with the copyright holder and legal officials in all copyright matters.

Email and Electronic Messaging

Best Practices and Encouraged Use

- Communicating and discussing business issues (whether normal or urgent priority) to inform others and obtain feedback or decision-making input.
- Involving only the users of the business who need to be informed or aware of the content and removed from any communications those who wish to opt-out due to their lack of involvement.
- Keeping messages brief and to the point to streamline communication and make it more efficient.
- Using the simple rules of who, what, when, where, and why to share details and answer any potential questions.
- Checking message content for accuracy and a good business writing style, such as proper grammar, spelling, and punctuation.
- Reading all messages and responding in a timely manner when requested or expected.
- Avoiding the Reply All function (which sends a response to all recipients of an email message) when not necessary or intended.
- Avoiding sensitive or confidential topics that should be addressed privately in person, if possible, or that may be inadvertently leaked if sent to the wrong recipients.
- Avoiding unnecessary communication, such as gossip or potentially critical remarks about coworkers.
- Avoiding unprofessional commentary which may be offensive or provocative.
- Making sure only authorized recipients are sent messages or attachments.
- Avoiding the sending of attachments (particularly large ones) when other methods of file sharing, such as internal networks, business file-sharing services, or external cloud services, could be utilized instead.
- Cleaning out old or unnecessary messages to reduce mailbox clutter and reserve email server storage.
- Report suspicious emails using the InfoSec IQ Red fish “Submit Email” tool

Prohibited Use

- Use of your organization-managed mail address for personal activities (including, but not limited to personal accounts on social networking services, loyalty/point club registrations, and above-listed prohibited activities) is prohibited.
- Organization-managed mail is company property. Users separating from Racine County shall not be permitted to take stored mail, calendar appointments, or contacts.

- IT staff may review users' email in the event of concerns regarding data or privacy breaches. Forewarning in this event is not guaranteed.
- Consider the content of email and intended recipient(s) before forwarding.
- Private information contained in email chains will not be forwarded to parties for which this information is out of scope for their role.
- Automatic/Mass forwarding of messages to parties/email addresses outside Racine County is prohibited.
- Do not transmit account credentials via email.
- Do not click on the links in suspicious email messages.
- Do not respond to spam or unsolicited offers from strangers (for example, alleged Nigerian princes, etc.)
- Use of email systems for sending of spam/malware/phishing emails.

CLEAR DESK AND CLEAR SCREEN

In order to reduce the risk of unauthorized access or loss of information, Racine County enforces a clear desk and screen policy as follows:

- Staff are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the work day.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left unsecured.
- Duo Multi-Factor Authenticator Security Tokens must not be left unsecured.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased or secured.
- Secure portable computing devices such as laptops, phones and tablets.
- Treat mass storage devices such as CD ROM, DVD or USB drives as sensitive and secure them in a locked drawer.

FLEXIBLE WORK

Racine County may allow staff the opportunity to work from home or other alternative worksites besides their Racine County office. Flexible work should be used when it is beneficial to both the staff and County operations.

- Flexible work arrangements are a workplace strategy, and not a right or benefit of employment.
- Flexible work arrangements will be granted or denied on a case-by-case basis at the discretion of the County, its departments, and supervisors.
- Flexible work arrangements must follow state and federal wage and hour laws, labor relations laws, and employment laws, as well as any collective bargaining agreements.
- Flexible work arrangements may not be used to create over-time hours unless overtime is approved in advance by a supervisor.
- Staff who agree to work certain hours as part of their flexible work arrangement must use those hours for Racine County work.
- All Racine County management and staff who participate in flexible work arrangements must be familiar with the contents of this policy and any other department-specific telework agreements.
- **The official worksite for staff participating in flexible work will be the site at which their business unit is located.**
- **Staff must complete all assigned work; remain available and in contact with the office, supervisors, and customers while teleworking; and be available to receive and respond to new work assignments and customer requirements while teleworking. In addition, if the needs of the office require a change in telework scheduling, staff agree to come into the office as directed.**
- **All timekeeping, leave, performance requirements, and special pay approvals are the same as for the traditional worksite. Staff agree to observe all policies with respect to absence and leave, compensatory time, and overtime, and properly document time and attendance records.**
- **Staff members agree to coordinate absences from the telework location, including official meetings, to ensure the supervisor can properly account for the whereabouts and attendance of teleworkers.**
- **Staff members must immediately notify the supervisor of any accident, injury, or illness occurring at the telework location.**

Flexible Work Categories

Routine Flexible Work refers to working from home or at an alternate work site when doing so better supports both a staff member's needs and the business needs of Racine County. It may be any ratio of office versus remote work. This may be as little as one day a year at the remote work site to as much as only one day a year at the office site.

Situational Flexible Work refers to flexible work situations that are the result of one time or irregularly occurring incidents such as inclement weather, system outages, natural disasters, other events, or issues as determined by the staff, supervisor, and/or Human Resources.

Compensation and Work Hours

The staff member's compensation, benefits, work status, and work responsibilities will not change due to participation in flexible work program. The amount of time the staff member is expected to work per day or pay period will not change as a result of participation in the program.

Eligibility and Considerations

Staff will be permitted for flexible work based on the suitability of their jobs, an evaluation of the likelihood of their being successful working flexibly, and the approval of their supervisor. Each department will make its own flexible work decisions and be responsible for measuring the success of the results. Before working flexibly, staff must read and sign this flexible work policy. Due to various job responsibilities, not all staff will be eligible to work flexibly. The IT department cannot support any telecommuter who has not signed this agreement. When evaluating flexible work solutions, it is important to evaluate criteria such as:

- Operational needs of Racine County
- The staff member's work duties
- The staff member's current and past job performance
- Positive and negative effects on customer service
- Availability of equipment, network, and workspace at the flexible work site
- Performance measures currently being used across the County
- Demonstrated work skills, such as time management, organizational skills, self-motivation, and the ability to work independently
- Reasonable accommodation requests should be approved under the Americans with Disabilities Act
- Pressing personal needs of the staff member that might benefit from a more flexible work arrangement, as long as the supervisor determines a flexible work arrangement will not harm the work unit, department, County, etc…

- Schedules of other staff or outside groups with whom the flexible work staff must coordinate
- Ability to work without the use of specialized equipment that may not be available or practical in the staff member's home (for example, large format plotters, color printers, etc.)
- Ability to adequately protect data privacy
- Ability to successfully interact with other staff and clients as required
- Other factors relevant to business needs

Equipment, Supplies, Hardware and Software

Equipment, hardware, software, and other supplies provided by Racine County remain the property of Racine County and are subject to the same business use restrictions as if located at a County office location. Home internet service and telephone line will remain the responsibility of the staff member. Racine County will not be responsible for operating costs, home maintenance, or any incremental or incidental costs whatsoever, associated with the use of the employee's residence of non-County office location. Racine County will not be responsible for damages to a staff member's personal or real property, during the course of performing official duties, or while using County equipment that occur at a telework location.

The flexible work staff will use and protect any Racine County provided equipment in accordance with Racine County's policies and procedures. Racine County equipment will be serviced and maintained by the appropriate County department and the flexible work staff must provide access to the equipment as needed for service during the work schedule periods or as pre-arranged scheduled maintenance.

County-owned software shall not be duplicated and must be protected. The flexible work staff is personally liable for the protection of information, software and other County data and property accessed directly or indirectly while performing duties as a flexible work staff member.

After any necessary equipment has been delivered, installed, and tested, a designated representative of Racine County may visit the flexible work staff member's site to inspect the workspace and, if needed install equipment.

Equipment supplied by the flexible work staff, if deemed appropriate by the organization, will be maintained by the flexible work staff. Racine County accepts no responsibility for damage or repairs to staff-owned equipment. Racine County reserves the right to make determinations as to appropriate equipment, subject to change at any time. Equipment supplied by the organization is to be used for business purposes only.

If the flexible work staff experiences internet, computer, or telephone outages, the staff must immediately contact their supervisor to assess the situation. After assessment, the flexible work staff may be required to report to the office site.

Flexible work staff are responsible to submit claims for County equipment stolen or damaged while in their homes to their personal insurance company and for filing a police report, if applicable, and any funds reimbursed for County property will be returned to Racine County. The supervisor should be contacted immediately in the event of any damage to or loss of County property and/or data.

Workspace

If required by the nature of the job, staff shall designate a workspace within the flexible work location for placement and installation of equipment to be used while working remote. Staff shall maintain this workspace in a safe condition, free from hazards and other dangers to the staff member and equipment. Any Racine County materials taken to the remote work location should be kept in the designated workspace and should not be made accessible to others.

If a designated workspace for flexible work is required by the nature of the job, Racine County has the right to make onsite visits (with 48 hours advance notice) to the remote workspace for purposes of determining that the site is safe and free from hazards, and to maintain, repair, inspect, or retrieve Racine County owned equipment, software, data, or supplies.

Security

All files, documents, records, and other materials created by the flexible working staff are property of the Racine County, just as they would be if created on a Racine County site. The staff and supervisor must ensure that appropriate safeguards are used to protect the security and confidentiality of such information, either by restricting certain information or records to the regular worksite or by providing appropriate physical, administrative, and technical security measures in the staff member's workspace.

Technical solutions like secure cloud services, encrypted communication, and VPN connections, among others, will be deployed as deemed necessary by Racine County, supervisor, and staff.

Staff are prohibited from disclosing any confidential, private or personal files, records, materials, or information. They may not allow any unauthorized parties to access corporate network or databases.

Staff members must follow the Government Data Practices Act, FTI, HIPAA, other data privacy legislation, and Racine County data privacy policies when working at any work site(s). Failure to do so may result in the loss of flexible work arrangement privileges and/or disciplinary action up to and including discharge. Violations may also result in criminal or civil litigation.

Staff members must handle protected information in a manner that avoids unauthorized disclosure. They should not read, discuss, display or expose protected information in common areas in their home or work site or in public places.

Staff members must manage records they create and maintain according to the appropriate record retention schedule.

Staff members must have a plan for disposing of protected information that follows the record retention schedule and avoids unauthorized disclosure.

Dependent Care

Flexible work is not a substitute for dependent care. Staff members must be free to perform their job responsibilities during the hours their work schedule requires. However, reasonable allowances can be made for dependent care in certain circumstances at the discretion of the staff member's supervisor as long as job performance is not affected and the staff member puts in a full day of work while handling dependent care responsibilities.

Communication and Meetings

Staff members must be available by telephone, videoconferencing, email, or other communication methods deemed necessary by Racine County, department, or supervisor during their scheduled work hours. Flexible work program participants must be available for in-person staff meetings at a Racine County site and other events deemed necessary by management.

Performance Evaluation

Staff members shall agree to participate in all studies, inquiries, reports, and analyses relating to the flexible program. Flexible work staff will be subject to the same performance evaluation criteria as other staff members at the applicable level.

A flexible work staff member and their supervisor must establish standards and expectations regarding work quality, quantity, and deadlines. They must also include a plan to monitor performance and measure productivity and results. Flexible work staff members must complete all assigned work, consistent with the standards, expectations, and measurements for all staff. The flexible work staff member and supervisor should establish a schedule to meet and review work progress, performance, and productivity while working remotely.

Organization Policies

Staff members remain obligated to comply with all other Racine County rules, practices, policies, and instructions while working flexibly from their remote workspace.

CYBERSECURITY INCIDENT RESPONSE PLAN

Excerpt:

Reporting

All Racine County staff have a responsibility to remain vigilant and protect the data stored within the systems we support. Any event that threatens the confidentiality, integrity, or availability of the information resources we support or utilize internally should immediately be reported to Information Technology Service Delivery

(Available 24/7). Service Delivery will evaluate a report, take action and escalate as required by Racine County policies and procedures, as well as our requirements under federal, state, and local laws/regulations.

Observers of the event should follow local emergency procedures. If life and safety are at immediate risk they should first act to ensure their own safety as well as the safety of staff, and then communicate when feasible. Dial 911 if there is any threat to life or a situation that requires an immediate response from police, fire or Emergency Medical Services (EMS) and follow Racine County's Emergency Response Plan.

Be a good observer and try to answer the following questions.

- What type of incident occurred?
- Where did the incident occur?
- When did the incident occur?
- How was it discovered?
- Who discovered it?
- Have any other areas been impacted, if known?
- What is the scope of the incident and who is it effecting, if known?
- Does it affect operations?

PASSWORDS

Excerpt:

Passwords	Frequency of Change	Disclaimers
User Level	90 Days	Cannot Reuse Previous 24 Passwords

Password Construction Requirements

Acceptable Methods to Create a Strong Password

- Be a minimum length of fourteen (14) characters in length, if a particular system will not support 14 character passwords, then the maximum number of characters allowed by that system shall be used.
- Must contain at least one upper case letter.
- Must contain at least one lower case letter.
- Must contain at least one number.
- Must contain at least one symbol.
- Must not start with a space.
- Must not contain username/full name/derivative of login.
- Must not be “single” dictionary words (ie/ Summer_2019).
- Must not be a derivation of a dictionary word (ie/ p@ssword, pass1word, pa$$word).

Password Composition to Be Avoided

- Avoid words, numbers, or known or public information associated with you (e.g. Social security numbers; Names, family names, pet names; birthdays, phone numbers, addresses; etc.).
- Avoid using your login name or any variation of your login name as your password. If your login is ‘fredrick’, do not use substitution or letter reordering. Examples would be ‘fr3dr1ck’, where the 3=e and the 1 (one)= i. Alternatively, do not use kcirderf (backwards) or add a digit to the beginning or end of the word (1fredrick or fredrick1).
- Avoid using the same character for the entire password (e.g., ‘11111111’) or using fewer than five unique characters.

- Avoid common letter or number patterns in your password (e.g., ‘12345678’ or ‘abcdefgh’). They are the first things hackers will test.
- When changing a password, change to an entirely new password. Do not just rotate through a list of favorite passwords.

Password Protection Standards

If someone demands a password, refer them to this document or have them call Racine County Information Technology Service Delivery at 262-636-3777.

If an account or password is suspected to have been compromised, report the incident to Racine County Information Technology Service Delivery at 262-636-3777, and change all passwords IMMEDIATELY!

Here is a list of “do not’s.”

- Do not keep default passwords, default passwords shall be changed immediately.
- Do not share passwords with anyone, including administrative assistants. All passwords are to be treated as sensitive and confidential information.
- Do not reveal a password over the phone to anyone, except authorized Racine County IT Service Delivery personnel.
- Do not reveal a password in an email message or other forms of electronic communication.
- Do not reveal a password to any coworker or your superior.
- Do not talk about or type a password in front of others.
- Do not hint at the format of a password (e.g., “my family name”).
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not use the "Remember Password" feature of applications.
- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY unencrypted computer system.
- Do not use the same password for access needs external to Racine County (e.g., online banking, benefits, etc.).

Remote Access Users

Access to the Racine County networks via remote access is to be controlled by using a Virtual Private Network (VPN) and a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.

Password Auditing and Logs

Password cracking or guessing may be performed on a periodic or random basis by Racine County or its delegates with the cooperation and support from the appropriate system administrator. If a password is guessed or cracked during one of these scans, the password user will be required to change it immediately. Racine County may also monitor for compromised passwords and will require users to change passwords if believed to be compromised.

Racine County will maintain a log of commonly used, predictable, or compromised passwords and update the log monthly and when organizational passwords are suspected to have been compromised directly or indirectly. These passwords will be added to a list of prohibited passwords in our active directory.

ACKNOWLEDGEMENT OF IT GENERAL EMPLOYEE POLICIES

This page is used to acknowledge the receipt of, and compliance with, Racine County's IT General Employee Policies.

Complete the following steps:

1. Read **all** the IT General Employee Policies.

2. Sign and date this form in the spaces provided below.

Signature

Your signature attests that you agree to the following terms:

I. I have received and read a copy of the Racine County's IT General Employee Policies, and I understand these policies and all their provisions.

II. I agree to act in accordance and compliance with all the policies' provisions.

III. I understand the organization may monitor the implementation of and adherence to these policies to review the results.

IV. I understand that violations of the IT General Employee Policies could result in termination of employment and/or legal action including civil and criminal prosecution.

Name:

Title:

Department/Location:

Employee Signature:

Date: