Trace Register – Information Security Policy

11/15/2025

I. Purpose and Scope

A. Purpose of the plan

This policy is to safeguard information systems within Trace Register, plan for events and prevent unauthorized access.

B. Scope

All systems, data, and services related to Information Technology.

II. Roles and responsibilities

A. Stakeholders with their contact information

Name	Role	Phone	Email
Zak Cobb	IT Director	206.539.6435	zcobb@traceregister.com
Bill Franceschine	VP of Technology	208.964.4986	bfranceschine@traceregister.com

III. Risk Assessment & Management

A. Risk Identification

- Identify potential risks, threats, and vulnerabilities related to information security.
- Consider internal and external factors that could impact Trace Register’s operations, data, and systems.

B. Risk Assessment

- Assess the likelihood and impact of identified risks.
- Prioritize risks based on severity and potential consequences.
- Use risk assessment methodologies (e.g., qualitative or quantitative) to evaluate risks.

C. Risk Documentation

- Document identified risks, including their descriptions, potential impact, and likelihood.
- Maintain a risk register or database to track risks over time.

D. Risk Mitigation and Strategies

- Develop strategies to mitigate or reduce identified risks.
- Assign responsibility for risk mitigation actions.
- Consider risk transfer (e.g., insurance) or risk acceptance when appropriate.

E. Risk Monitoring and Review

- Regularly review and update risk assessments.
- Monitor changes in the threat landscape and adjust risk management strategies accordingly.
- Ensure ongoing risk awareness and communication within the organization.

IV. Vulnerability Assessment & Management

A. Regular Vulnerability Assessment:

- Conduct regular vulnerability assessments of both software applications and infrastructure components.
- Use automated tools (e.g., vulnerability scanners) to identify vulnerabilities.
- Schedule assessments periodically (e.g., monthly or quarterly) and after significant changes.

B. Software Vulnerabilities

- Focus on identifying vulnerabilities in software applications, including web applications, databases, and custom-developed software.
- Consider the following:

  a) Known software vulnerabilities (CVEs)
  b) Misconfigurations
  c) Weaknesses in authentication mechanisms
  d) Insecure coding practices

C. Infrastructure Vulnerabilities:

- Assess vulnerabilities in network devices, servers, and other infrastructure components.
- Look for outdated firmware, default credentials, and open ports.
- Consider both internal and external infrastructure.

D. Patch Management:

- Develop a patch management process:

  a) Identify critical patches based on severity and impact.
  b) Test patches in a non-production environment before deployment.
  c) Deploy patches promptly to minimize exposure to vulnerabilities.
  d) Monitor vendor security advisories and apply patches accordingly.

E. Emergency Patching:

- Address critical vulnerabilities (e.g., zero-day vulnerabilities) promptly.
- Implement emergency patches as soon as they become available.
- Communicate urgent patching requirements to relevant teams.

F. Vulnerability Remediation:

- Assign responsibility for addressing identified vulnerabilities.
- Prioritize remediation efforts based on risk assessment.
- Document remediation actions and track progress.

G. Continuous Monitoring:

- Continuously monitor for new vulnerabilities.
- Subscribe to security mailing lists and follow security news.
- Stay informed about emerging threats.

V. Change Management

A. Change Request Process:

- Changes should be submitted to IT for prioritization.
- IT management will define the required information for a change request, including the reason for the change, impact assessment, and proposed solution.
- Anyone can submit a change

B. Change Approval Workflow:

- Involve relevant stakeholders (e.g., IT management) in the approval process.
- Ensure that changes align with business goals and security requirements.

C. Documentation:

- Document all changes, regardless of their size or impact.
- Include details such as the date of the change, the person responsible, and the affected systems.
- Maintain a change log or repository.

D. Testing and Validation:

- Require testing for all changes before implementation.
- Test changes in a controlled environment (e.g., staging or test environment) to identify potential issues.
- Validate that the change achieves its intended purpose without adverse effects.

E. Emergency Changes:

- Define criteria for emergency changes (e.g., critical security patches, system failures).
- Expedite emergency changes while ensuring proper documentation.
- Conduct post-implementation reviews for emergency changes.

F. Backout Plans:

- Develop backout plans for each change.
- Specify the steps to revert to the previous state if a change causes unexpected problems.
- Communicate backout procedures to relevant teams.

G. Communication:

- Notify affected parties about upcoming changes.
- Provide advance notice to minimize disruption.
- Communicate the expected impact and any required actions (e.g., user training).

H. Change Records:

- Maintain a central repository for change records.
- Include information on successful changes, unsuccessful changes, and lessons learned.
- Use this repository for auditing and accountability.

VI. Data Classification

A. Data Categorization:

- Public Data:

  a) Information that is publicly available and does not require protection.
  b) Examples: Marketing materials, press releases, public website content.

- Confidential Data:

  a) Sensitive information that requires protection against unauthorized access.
  b) Examples: Employee records, financial data, internal memos.

- Sensitive Data:

  a) Data that, if disclosed, could harm individuals or the organization.
  b) Examples: Personally identifiable information (PII), trade secrets.

- Highly Sensitive Data:

  a) Extremely critical data that demands the highest level of protection.
  b) Examples: Intellectual property, encryption keys, strategic plans.

B. Handling Guidelines:

- Public Data:

  a) No special handling requirements.
  b) Accessible to the public.

- Confidential Data:

  a) Access restricted to authorized personnel.
  b) Encrypt data in transit and at rest.
  c) Implement access controls (e.g., role-based access).

- Sensitive Data:

  a) Limit access to individuals with a legitimate need.
  b) Use strong encryption for storage and transmission.
  c) Monitor access and audit logs.

- Highly Sensitive Data:

  a) Restricted access to a select few.
  b) Require multi-factor authentication (MFA).
  c) Regularly review and update access permissions.
  d) Utilize data loss prevention (DLP) solutions.

C. Data Retention and Destruction:

- Regularly review and delete data that is no longer needed.
- Follow secure data destruction practices (e.g., shredding physical documents, secure wiping of digital storage).

D. Employee Training:

- Educate employees on data classification and handling.
- Ensure that employees understand their responsibilities based on data sensitivity.
- Conduct periodic training sessions.

VII. Backup Procedures

A. Backup Frequency:

- Regular Backups:

    a) Schedule regular backups of critical data (e.g., databases, configuration files).
    b) Determine the appropriate frequency (e.g., daily, weekly) based on data volatility and business needs.

- Incremental Backups:

    a) Use incremental backups to capture changes since the last full backup. This will reduce backup, transfer, and storage requirements.

- Full Backups:

    a) Perform periodic full backups to ensure a complete copy of data can be stored.

B. Data Retention Policies:

- Retention Periods:

    a) Data is retained based on business, client, and regulatory requirements.
    b) Review retention periods periodically with management.

- Archival Backups:

    a) Some backups are archived for long-term retention.
    b) Archival backups are to be stored securely (e.g., encrypted and in a separate location).

C. Backup Storage and Locations:

- Offsite Backups:

    a) Store backups offsite to protect against physical disasters (e.g., fire, flood).
    b) Use cloud storage or remote data centers.

- Onsite Backups:

    a) Maintain onsite backups for faster recovery.
    b) Ensure physical security of onsite backup storage.

- Redundancy:

    a) Use redundant backup locations to prevent a single point of failure.
    b) Implement the 3-2-1 backup strategy (3 copies, 2 different media, 1 offsite).

D. Backup Testing and Verification:

- Regular Testing:

  a) Test backup restoration processes periodically.
  b) Verify that backups are complete and accurate.

- Test Recovery Scenarios:

  a) Simulate disaster scenarios (e.g., server failure, data corruption).
  b) Ensure that backups can restore systems to a functional state.

- Document Procedures:

  a) Document step-by-step procedures for backup restoration.
  b) Include contact information for key personnel involved in recovery.

E. Automated Backup Solutions:

- Backup Software:

  a) Use reliable backup software to automate backup tasks.
  b) Set up alerts for backup failures.

- Snapshot Backups:

  a) Leverage snapshot technology for virtual machines and cloud-based systems.

F. Monitoring and Reporting:

- Backup Monitoring:

  a) Monitor backup jobs and logs.
  b) Address any failures promptly.

- Backup Reports:

  a) Generate regular backup reports. Include information on successful backups, failures, and storage usage.

VIII. Remote Access

A. Secure Remote Access Guidelines:

- VPN (Virtual Private Network):

  a) Employees are required to use VPNs when accessing internal resources.
  b) VPNs can be used to tunnel remote worker internet connections.

- Multi-Factor Authentication (MFA):
  a) Enforce MFA for all interactive remote access sessions (e.g., RDP, SSH, web portals).
  b) Non-interactive VPN sessions may be established using strong certificate-based authentication, including user-specific certificates, without requiring MFA.

a) Enforce 2FA for remote access.
b) Use a combination of something the user knows (password) and something the user has (e.g., mobile app, hardware token).

- Access Control Lists (ACLs):

a) ACLs are defined and maintained to restrict remote access to specific IP addresses or ranges.
b) Whitelist authorized IP addresses and block others.

- Remote Desktop Protocol (RDP):

a) Limit RDP access to authorized users.
b) Change the default RDP port to avoid automated attacks.
c) Use Network Level Authentication (NLA) and 2FA for RDP sessions.

- Secure Shell (SSH):

a) Use SSH for secure remote access to servers.
b) Disable SSH root login and use individual user accounts.
c) Implement key-based authentication instead of password-based authentication.

B. Encryption and Data Protection:

- Data Encryption:

a) Encrypt data transmitted during remote access.
b) Use secure protocols like TLS (Transport Layer Security) (for web applications and VPNs).

- Endpoint Encryption:

a) Require full-disk encryption on remote devices (laptops, mobile devices).
b) Encrypt sensitive files and folders.
c) Use BitLocker (Windows), FileVault (macOS), or similar.

- Data Loss Prevention (DLP):

a) We have Implemented DLP solutions to prevent accidental data leaks.
b) We will monitor and block sensitive data transfers.

C. Remote Work Policies:

- BYOD (Bring Your Own Device):

a) Personal devices need to be approved by the manager.
b) Approved endpoint protection must be installed.
c) Multifactor (MFA) authentication is required to access Trace Register Systems.

- Secure Wi-Fi:

a) Employees should always connect to secure Wi-Fi networks.
b) Avoid public Wi-Fi networks for sensitive work.
c) Use a VPN when connecting to public Wi-Fi.

- Certificate-Based VPN Monitoring:
a) All certificate-based VPN sessions must be logged and monitored for anomalies. Alerts should trigger if a certificate is revoked or expired.

E. Certificate Lifecycle Management:
- Define certificate issuance, renewal, and revocation processes. Certificates should be tied to user identity and device, and revoked immediately upon termination or device compromise.

D. Monitoring and Auditing:

- User Activity Logs:

a) Log remote access events (successful logins, failed attempts).
b) Regularly review logs for suspicious activities.

- Behavioral Analytics:

a) Use behavioral analytics tools to detect anomalies in remote access behavior.
b) Identify unusual patterns (e.g., multiple failed login attempts).

IX. Physical Security & Access Control

A. Access Control:

- Access Groups:

a) Systems Administrators
b) IT Management
c) Datacenter Technicians

- Badge Systems:

a) Employee badges for physical access to datacenter location.
b) Revoke access promptly when an employee leaves the organization.

Biometrics and Smart Cards:

a) Biometric authentication (fingerprint, retina scan) is required for secure access to datacenter.

B. Security Audits and Inspections:

- Regular Assessments:

a) Conduct periodic security audits.
b) Evaluate physical security measures for effectiveness.

- Third-Party Reviews:

a) Consider external security consultants for unbiased assessments.
b) Address any identified vulnerabilities promptly.

C. Cybersecurity Integration:

- Secure Network Infrastructure:

a) Ensure network switches, routers, and servers are physically secured.
b) Limit access to network closets and data centers.

X. Logical Security & Access Control

Definition: Interactive login refers to sessions where a user actively enters credentials (e.g., desktop login, RDP, SSH, web portal). Non-interactive sessions (e.g., automated VPN tunnels) do not involve manual credential entry and may use strong certificate-based authentication.

A. User Authentication:

- Strong Authentication:

  a) Require multi-factor authentication (MFA) for user logins.
  b) Use a combination of something the user knows (password), something the user has (token or phone), and something the user is (biometrics).
  c) Implement time-based one-time passwords (TOTP) or hardware tokens.

- Password Policies:

  a) Enforce strong password policies:

    i) Minimum length (8)
    ii) Complexity (mix of uppercase, lowercase, numbers, and special characters)
    iii) Regular password changes (90 days)
    iv) Password history (prevent reuse of recent passwords)

- Account Lockout:

  a) Implement account lockout mechanisms to prevent brute-force attacks.
  b) Lock user accounts after repeated failed login attempts.

B. Authorization Mechanisms:

- Role-Based Access Control (RBAC):

  a) Assign roles to users based on their job responsibilities.
  b) Users inherit permissions based on their assigned roles.

- Attribute-Based Access Control (ABAC):

  a) Use attributes (e.g., user attributes, resource attributes) to make access control decisions.
  b) Define policies based on attributes (e.g., department, location, time of day).
  c) ABAC allows fine-grained access control.

- Least Privilege Principle:

  a) Grant users the minimum permissions necessary to perform their tasks.
  b) Regularly review and adjust permissions based on job changes.
  c) Avoid granting excessive privileges.

- Certificate-Based Authorization:

    a) For non-interactive sessions (e.g., automated VPN tunnels), access decisions must rely on strong certificate-based authentication tied to user identity and device.
    b) Certificates must comply with organizational PKI standards and be revoked immediately upon termination or device compromise.
    c) Certificate-based access must still adhere to RBAC and ABAC policies to ensure least privilege.

C. Database Access Control:

- Database Roles and Permissions:

    a) Create database roles (e.g., read-only, read-write) based on user responsibilities.
    b) Assign permissions to roles rather than individual users.
    c) Limit direct access to sensitive database tables.

- Stored Procedures and Views:

    a) Use stored procedures and views to encapsulate database logic.
    b) Limit direct SQL access to prevent unauthorized data manipulation.
    c) Implement parameterized queries to prevent SQL injection.

D. Application Security:

- Input Validation:

    a) Validate user input to prevent injection attacks (e.g., SQL injection, cross-site scripting).
    b) Sanitize input data before processing.

- Session Management:

    a) Implement secure session management:

        i) Use secure cookies.
        ii) Set session timeouts.
        iii) Invalidate sessions after logout or inactivity.

- API (application programming interfaces) Security:

    a) Secure APIs (application programming interfaces) with authentication (e.g., OAuth, API keys).
    b) Validate API requests.
    c) Rate-limit API calls to prevent abuse.

E. Audit Trails and Monitoring:

- Audit Logs:

  a) Log user access, authentication events, and authorization decisions.
  b) Retain logs for a specified period.
  c) Regularly review logs for suspicious activities.

- Intrusion Detection and Prevention:

  a) Implement intrusion detection systems (IDS) and intrusion prevention systems (IPS).
  b) Monitor network traffic and system logs for signs of unauthorized access.
  c) Set up alerts for suspicious behavior.

XI. Privacy Expectations

A. User Privacy Protection:

- Compliance with Regulations:

  a) Ensure compliance with relevant privacy regulations.
  b) Understand the legal requirements related to user privacy and data protection.

- Consent and Transparency:

  a) Obtain informed consent from users before collecting their personal data.
  b) Clearly communicate the purpose of data collection and any sharing practices.
  c) Provide a privacy policy that explains how user data is handled.

- Data Minimization:

  a) Collect only the minimum necessary personal data for the intended purpose.
  b) Avoid unnecessary data collection or retention.

- Anonymization and Pseudonymization:

  a) Anonymize or pseudonymize user data whenever possible.
  b) Use unique identifiers instead of directly identifying information.

- Sensitive Data Handling:

  a) Treat sensitive personal data (e.g., health records, financial information) with extra care.
  b) Implement additional security measures for sensitive data.

- Data Breach Response:

  a) Have a data breach response plan in place.
  b) Notify affected users promptly in the event of a breach.
  c) Cooperate with regulatory authorities as required.

B. Safeguarding Personal Data:

- Encryption:

  a) Encrypt personal data during transmission (e.g., HTTPS) and storage (e.g., encrypted databases).
  b) Use strong encryption algorithms and key management practices.

- Access Controls:

  a) Limit access to personal data to authorized personnel only.
  b) Implement role-based access controls (RBAC).
  c) Monitor access logs for suspicious activity.

- Data Retention Policies:

  a) Retain user data for 3 years, unless otherwise specified.
  b) Regularly review and delete data that is no longer necessary.

- User Rights:

  a) Respect user rights (e.g., right to access, right to be forgotten).
  b) Provide mechanisms for users to exercise their rights.
  c) Handle user requests promptly.

C. Privacy by Design:

- Incorporate Privacy Early:

  a) Consider privacy implications during system design and development.
  b) Embed privacy controls into the architecture.

XII. Employee Agreement

A. Policy Acknowledgment:

- All employees with access to IT systems must read and acknowledge their understanding of this information security policy.
- Upon joining the organization, new employees should receive training on the policy.
- Acknowledgment can be in the form of a signed document or an electronic confirmation.

B. Compliance Expectations:

- Employees are expected to adhere to the policy.
- Compliance includes following the procedures outlined in the policy, reporting security incidents promptly, and cooperating with security audits.

C. Regular Training and Updates:

- Security awareness training sessions should be available for employees.
- Employees will be informed about any updates or changes to the policy.

D. Reporting Violations:

- Employees should report any suspected violations of the policy.
- Encourage a culture of accountability and responsibility.

E. Consequences of Non-Compliance:

- Depending on the severity, consequences may include verbal warnings, written warnings, suspension, or termination.