IT Service & Software Policy

1. Purpose

The purpose of this policy is to establish guidelines for the operation, management, and monitoring of third-party hardware, software, and services on Brookings County's network and hardware. This policy aims to minimize the risk of new services and ensure that any services added are monitored, justified, and secure.

2. Scope

This policy applies to all employees, departments, contractors, vendors, and any other third parties who have access to the organization's network and systems. It covers all requests for the addition of any software, hardware, or services including those for applications, services, and remote access.

3. Policy Statements

3.1 Authorization and Justification

- All requests for new services must be submitted in writing and include a detailed justification for the access.

- Requests must be approved by IT and the relevant Department Head before any implementation can occur.

- The justification must include the purpose, any hardware or software requirements, anticipated implementation timeline, vendor contact information, and network connection requirements to implement the service (if applicable).

3.2 Security Assessment

- Before approving the implementation of a new service, IT will conduct a risk assessment to evaluate potential security vulnerabilities.

- External access to the network will only be allowed if there are no viable alternatives, such as using a VPN or secure tunneling methods. If external access is required, the Requesting Party must provide justification for this access, alternative methods investigated, length of required access, and IPs or IP ranges to provide access to.

- Before additional hardware can be deployed, IT must be informed of its proposed location, purpose, and installed software. Failure to disclose remote access tools on new services may result in disruption of service.

- Any evidence of a service impacting the stability, speed, or availability of the network may be disabled with or without notice.

- Outbound data must not contain any more data than what is needed to maintain the service. Services found to be collecting data from the network not related to the operation of the software/service may be disabled with or without notice. Activities including, but not limited to, collecting network infrastructure data, server data (including network shares and services), network sniffing, penetration testing, spoofing of services, or allowing unapproved persons access to the network is prohibited unless explicitly authorized by IT and the Brookings County Commission Department.

- Notices of exploits in the software or services providing the content may result in the service being blocked without notice until remediation is made, or the vulnerability is determined to be not applicable.

- Installed hardware or software must not be directly or indirectly sourced from a "Prohibited Entity," as defined in South Dakota Codified Law 5-18A-1 (19A).

3.3 Service Management

- IT will maintain a log of all external services in use on the County network(s), including details such as the date installed, justification, approved duration, requesting entity, and allowed external IP addresses (if applicable).

- Services must be reviewed at least annually to ensure they are still required. Services no longer in use or needed will be disabled.

- Failure to confirm that a service is still in use or needed may result in any adjustments made for its use being discontinued. If a service is discontinued in this way a new security assessment will need to be made.

3.4 Monitoring and Auditing

- Computers accessing this service will be monitored for unusual activity through enhanced logging. Logs indicating unusual activity will be submitted to the vendor to verify legitimate activity. If activity is illegitimate or if the vendor declines to respond within a reasonable amount of time, the service may be disabled.

- Contact information for the hardware or service provider will be provided to IT and kept on file.

- If a centralized logging platform is not in use, logs must be accessible by IT staff either directly or through a request with the service provider.

- If additional hardware or software is required to adequately monitor these services, service implementation may be delayed until such technology is acquired. This acquisition may be at the expense of IT or shared with the requesting party, depending on applicability to other portions of the IT infrastructure.

- Devices or services found to be evading monitoring may be blocked with or without notice.

3.5 Compliance

- Failure to comply with this policy may result in the services being disabled or blocked with or without notice. If services are discontinued in this way a new security assessment may need to be made.

3.6 Security Incidents

- Any security breaches or incidents involving services or software provided by a third party must be reported immediately to IT. If such an incident occurs, the server may be disconnected from the network until an assessment can be made to determine if there is evidence of a compromise and, if so, remediate it. Remediating the issue does not mean that the service will be enabled again.

- Failure to report an incident will result in the immediate discontinuation of that service.

4. Determinations

4.1. Decision-Making Criteria

- Decisions will be made using a risk-based approach. IT will determine whether the benefits of allowing the service outweigh the potential risks, considering the effectiveness and potential cost of proposed mitigations.

- If the risks are deemed acceptable and necessary safeguards are in place, the request may be approved.

- If the risks are determined to be too high or cannot be adequately mitigated, the request may be denied, or alternative solutions should be investigated.

4.2. Appeals

- If a department disagrees with the determination of IT they may appeal that decision. IT will re-evaluate the solution and determine if anything was missed in the initial assessment of the service.

- If the request continues to be denied the department may request mediation to determine what, if anything, can be done to allow for implementation of the service.

- If a request is denied the department must wait 6 months before making another request for the same service.

5. Roles and Responsibilities

- IT: Responsible for evaluating and approving service additions to the County network infrastructure, conducting risk assessments, maintaining logs, monitoring services, and the technical implementation of feature additions to the county computer infrastructure.

- Requesting Party: Must provide a clear justification for the request and ensure compliance with security requirements. If alternative methods of content delivery were evaluated the requesting party must also provide those options and reasoning for rejection.

- Vendor: Must provide a list necessary protocols/ports involved in implementation of the system, target IP addresses, and if firewall changes need to be made. The vendor must maintain an event log history of at least 30 days indicating connection attempts, connection outcomes, and transaction logs. The vendor must also follow any State or Federal laws or regulations regarding the implementation, access, and security of the system.

6. Review and Revision

This policy will be reviewed annually or as required in response to changes in technology, regulatory requirements, or security risks.

Approved this 1st day of October, 2024.

Larry Jensen, Chairperson
Brookings County Commission