Type of Policy: Administrative
Effective Date: February 2024
Last Revised: February 2024
Review Date: February 2025
Policy Owner: Georgia Tech CyberSecurity
Contact Name: John Karrh
Contact Title: Governance Risk & Compliance Manager - Cyber Security
Contact Email: johnkarrh@gatech.edu

Reason for Policy:
The Georgia Institute of Technology (Georgia Tech) Ransomware Protection Policy (RPP) provides guiding principles for Information Technology (IT) administrators at Georgia Tech to prevent the infection, spread, and distribution of ransomware on the Georgia Tech network.

Scope:
All users (including all employees and students) of Georgia Tech IT resources and all IT resources belonging to Georgia Tech are covered by this policy.

Policy Statement:
Effective protection against ransomware should follow industry best practices for cybersecurity protection, outlined in the NIST Cybersecurity Framework 2.0. NIST's guidelines outline 6 high level categories of controls:

1. Govern
2. Identify
3. Protect
4. Detect
5. Respond
6. Recover

In order to effectively protect against ransomware, appropriate controls need to be applied at each category.

Procedures:
Georgia Tech will be referred to as 'the organization' throughout the policy document.

Govern

- Establish a comprehensive cybersecurity strategy to govern the cybersecurity program, covering the organization's current cybersecurity posture, and the goal state. This should include understanding the business' needs and the goals of the organization in order to effectively determine critical systems and assets. This should prepare the organization to determine what level of risk is appropriate for the system and which controls should be implemented.

    - As a part of this strategy, determine organizational risk appetite and track residual risk against these benchmarks in order to ensure the organization's risk is in line with the defined risk appetite.
    - The risk appetite, residual risk, and the risk management strategy should be re-evaluated at least annually to ensure that it remains accurate for the organization.
    - Risk assessments must be performed at least annually or when major system changes occur in order to determine what the residual risk of the system is and where there are control gaps that need to be addressed.
    - Legal, regulatory, and contractual cybersecurity obligations should be reviewed to ensure that appropriate levels of cybersecurity controls are applied to the appropriate data and systems
- Purchase appropriate levels of cyber insurance which covers ransomware attacks.
- Establish appropriate security policies, procedures, and processes and ensure they are communicated throughout the organization, as well as being enforced when appropriate.
    - Policies, procedures, and documentation must be regularly reviewed in order to address emerging threats and new changes in technology, as well as organizational changes and risks.
- All open-source and third party software, hardware, and services must be reviewed and approved by the third party risk management team before it can be used. This includes an evaluation of the software's development process, security vulnerabilities, and available support.
- Ensure that roles and responsibilities related to cybersecurity, and ransomware protection are well understood and integrated into job descriptions throughout the organization.

Identify

- Establish and maintain a comprehensive asset and application inventory which includes asset and application owners in order to understand the organization's footprint.
    - Assets should be tagged with their level of criticality (based on the highest sensitivity data processed by that system or by risk to the organization if it is rendered unavailable).
    - Assets and data should be tracked throughout their lifecycle, updating the classification as necessary, until the assets are retired. This ensures that all assets are accounted for and protected so that there is no unprotected node to the network.
- Classify all data according to the highest level of appropriate classification based on the Georgia Tech Data Protection Categorization and ensure all data has an assigned data steward responsible for its classification and protection.
- Threat intelligence sources must be consulted regularly (including relevant government sources like CISA bulletins and information sharing groups (like the

ISACs)) in order to stay up to date on common attack vectors used in ransomware attacks.
- Regular vulnerability scans must be performed in order to identify and validate known vulnerabilities present in the system (these vulnerabilities should be regularly patched as outlined in the 'protect' section in order to prevent their exploitation by ransomware operators).
- All changes to the system must follow the defined change management process in order to ensure vulnerabilities are not introduced into the system and all changes are tracked to identify unusual network behavior.
    - Any exceptions to this, or other policies must be tracked and approved by the policy owner.
- Regular penetration tests should be performed in order to proactively identify vulnerabilities in the system which could be exploited by a ransomware operator.
- Regular table top exercises must be held in order to ensure stakeholders are aware of their roles and responsibilities as outlined in this policy, and are prepared to take appropriate actions if an incident occurs.
    - Lessons learned from these exercises should be tracked in order to ensure processes and systems are continuously improved.
    - Decisions made in these exercises should be documented (such as whether to pay a ransom or when a ransom should be paid) in order to guide decision makers during a real ransomware incident.

Protect

- All systems must be regularly updated and patched to prevent exploitation of known vulnerabilities.
    - Follow all appropriate Georgia Tech Cyber Security Standards which address this control, such as the Web Server Standard and the Vulnerability Management Standard
- All key data must be regularly backed up in an immutable data store.
    - Follow all appropriate Georgia Tech Cyber Security Standards which address this control, such as the System Administration Responsibilities Standard
- Regular recovery testing must be performed in order to ensure that key data backups are effective and that they meet recovery time objectives in order to ensure that if primary data stores are impacted by a ransomware attack, the organization can effectively restore from backups and resume operations.
- Systems that are no longer needed must be appropriately retired in order to ensure they do not present easy access for malicious attackers.
- Mandatory security awareness training must be provided to all employees in order to ensure they are aware of the dangers of common ransomware delivery mechanisms like phishing emails and understand how to report suspicious activity to the cybersecurity team.

- Appropriate endpoint protection measures must be leveraged such as hardening standards based on industry frameworks and antivirus software should be installed on all university-owned devices.
    - Follow all appropriate Georgia Tech Cyber Security Standards which address this control, such as the SSH Server Standard and the Vulnerability Management Standard
- Access control policies must be regularly audited and updated in order to ensure they follow least privilege principles and that privilege creep (as users transition between jobs at the same organization and continue to accumulate privileges) is prevented, in order to limit the access of users in order to ensure that if a user account is compromised, the blast radius is limited.
- Strong authentication methods must be leveraged (including multi factor authentication (MFA)) and the standards outlined in the Georgia Tech Password Policy must be followed.
- Egress and ingress points to the network must be secured by leveraging firewalls, spam filters for email, and data loss prevention solutions to prevent malicious actors from gaining network access, sending phishing emails to users, and exfiltrating stolen data from the network.
    - Follow all appropriate Georgia Tech Cyber Security Standards which address this control, such as the Network Firewall Standard
- Appropriate physical security measures must be implemented to prevent malicious attackers from gaining direct access to servers or other physical infrastructure.
- All data should be encrypted both in transit and at rest using industry standard encryption algorithms so that unencrypted data is not able to be accessed by an unauthorized user.
- Encryption keys should be centrally managed and stored in a secure manner, such as a hardware security module (HSM) or a cloud key management service (KMS).
- Block portable USB devices and other removable media as they are a common method of initial infection.

Detect

- Perform regular inspections of Georgia Tech's IT infrastructure to ensure unauthorized physical access has not occurred.
- The approved endpoint detection and response tool must be installed on all corporate IT devices to identify and quarantine potentially infected systems quickly.
    - Follow all appropriate Georgia Tech Cyber Security Standards which address this control, such as the Approved Endpoint Software Standard and the System Administration Responsibilities Standard
- All relevant logs from all system assets and applications should be centrally logged and stored in a security information and event management (SIEM) tool in order to provide early detection of attacks.

    - Logs should be retained for a minimum of 6 months to ensure the ability to review logs for an appropriate period of time.
- Custom alerts must be created in the SIEM in order to detect suspicious activity (such as network and system anomalies, unusual user behavior, indicators of compromise, or other adverse events), identify incidents as early as possible, and prevent the spread of malware, particularly ransomware.
- An intrusion prevention system or an intrusion detection system must be installed to monitor network traffic for signs of an attack, and take action to prevent them from spreading (in the case of an intrusion prevention system).

Respond

- The security incident response team will investigate alerts in order to determine if an incident has occurred and will follow defined playbooks in order to respond to a confirmed incident (which define steps to be followed in the case of an incident).
    - Incidents must be classified according to their severity and the appropriate playbook followed, including logging all activity taken to investigate the incident.
    - Data related to an incident or infection must be collected using forensic incident response best practices. If necessary, third party forensic incident responders should be leveraged in order to ensure the correct collection of incident data for reporting to law enforcement.
    - Incident response playbooks must be regularly reviewed and updated in order to ensure the incident response team is ready to respond to a suspected incident quickly.
    - Identify the root cause of the incident in order to hold an effective lessons learned session after the incident, and ensure that all impacted systems have been identified and quarantined.
- A pre-established communication plan must be used to keep internal and external stakeholders informed of the status of the ransomware incident, outside of normal communications bands, if necessary.
    - Notify impacted parties and/or law enforcement agencies as appropriate.
    - Ensure that there are defined spokespersons to handle the media and public releases, if appropriate.
- Any infected systems must be quarantined from the network in order to contain the incident from spreading. Eradication measures should be taken to remove the malware from the system, such as full system wipes of impacted devices.

Recover

- The Chief Legal Officer must be consulted if a ransom is requested, in order to ensure that all legal and ethical implications have been considered, and to ensure appropriate communication channels with law enforcement agencies and cyber insurers have been opened.

    - The pre-established communication plan should be used to keep relevant stakeholders apprised of the situation. The Chief Communications Officer (CCO) should be involved at each step, and the CCO or a delegate should be responsible for any public updates.
    - If required, a ransomware negotiator should be employed to assist in the ransom negotiation process, as well as in provisioning bitcoin or other cryptocurrencies leveraged to pay a ransom.
- All containment and eradication measures must be complete before any recovery procedures are followed:
    - Immutable backups must be used to restore any encrypted or damaged files after ensuring the network is completely free of ransomware or other infection.
    - All malware must be confirmed to have been removed from quarantined devices before they are re-connected to the network.
    - Inspect and test all the devices to ensure successful system restoration.
- A lessons learned review of any incidents must be held to address the following:
    - Based on the root cause of the incident, new controls should be recommended to prevent the same type of incident from occurring again.
    - Implement the recommended controls in order to remediate the identified gaps.
    - Evaluate the effectiveness of the incident response plan and playbooks in order to identify any gaps and remediate them.
    - Identify any other gaps in policies, procedures, and other documentation, and remediate the gaps.

Roles and Responsibilities:

Chief Information Security Officer

The Chief Information Security Officer (CISO) is responsible for overseeing the implementation and maintenance of a ransomware prevention program, as well as the relevant policies. Additionally, the CISO, or a delegate, is responsible for the investigation and response to cybersecurity incidents. Cybersecurity incident response will be coordinated with all appropriate parties.

Incident Captain

The incident captain is responsible for being the lead on a cyber incident, for ensuring appropriate investigative steps are followed, and for ensuring that all appropriate parties are consulted where appropriate.

Incident Responders

Incident responders are responsible for detecting and responding to incidents.

IT Administrators

IT Administrators are responsible for following the standards outlined in Georgia Tech's technical policies and standards for the systems which they administer.

Chief Legal Officer

The Chief Legal Officer (CLO) is responsible for determining whether or not a ransom should be paid and whether or not the organization is in compliance with all relevant regulations when determining the legality of paying such a ransom. The CLO is also responsible for owning communications between law enforcement agencies and the organization, as well as the relationship between the organization and their cyber insurer. Additionally, the CLO is responsible for communicating the implications of a ransomware incident on any contractual or other legal obligations to all appropriate parties.

Chief Communications Officer

The Chief Communications Officer (CCO) is responsible for developing and overseeing a communication plan to inform internal and external stakeholders of relevant updates during a cyber incident.

Users of Georgia Tech IT Infrastructure

If a Georgia Tech user suspects that a ransomware incident has occurred, they should report the incident directly to the Georgia Tech Cyber Team as outlined in the Cyber Security Policy. Users can contact the Security Operations Center (SOC) at 404.385.CYBR (2927) or soc@gatech.edu.[1]

Policy Terms:

Ransomware - a type of malicious software that encrypts software and requests a ransom to be paid for the decryption key

"Security Incident – A security incident is an event, as determined by Georgia Tech Cyber Security, that violates an applicable law or Institute policy including the violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An incident could also be established based on the

[1] Paraphrased from - Georgia Tech. "Incident Response – Georgia Tech Cyber Security." *Georgia Tech Cyber Security*, Unknown, https://security.gatech.edu/incident-response/. Accessed 11 February 2024.

potential for harm to the confidentiality, integrity, or availability of Georgia Tech IT resources."[2]

Exceptions:

Any deviations from this policy should be reviewed via the Information Security Exception Review process, as outlined in the Policy Exceptions Policy.

Enforcement:

All users who are covered by this policy are expected to adhere to this policy. Violations of the policy can result in loss of system or network privileges, administrative sanctions (including termination or expulsion), as outlined in the appropriate Georgia Tech disciplinary policies, as well as personal civil and/or criminal liability, where appropriate.

Policy History

Version	Revision Date	Author	Description of Changes
1.0	February 11, 2024	Team 19	New Policy

[2] Georgia Tech. "Incident Response – Georgia Tech Cyber Security." *Georgia Tech Cyber Security*, Unknown, https://security.gatech.edu/incident-response/. Accessed 11 February 2024.

References:

1. Georgia Tech. “Incident Response – Georgia Tech Cyber Security.” *Georgia Tech Cyber Security*, Unknown, https://security.gatech.edu/incident-response/. Accessed 11 February 2024.
2. “Security Operations Management Tool.” *Georgia Tech Cyber Security*, security.gatech.edu/security-operations-management-tool/. Accessed 15 Feb. 2024.

Recommended Changes to GT's IT Policies

We recommend adding the 'Ransomware Policy' to the 'related information' links at the bottom of each of these policies.

- Acceptable Use Policy
- Controlled Unclassified Information
- Credit Card Processing
- Cyber Security Policy
- Data Governance and Management Policy
- Data Privacy Policy
- Data Resources
- Email Forwarding for Life
- GLBA Information Security Program
- Identity Theft Prevention Policy
- Information Technology Accessibility Policy
- Institution Online Resource Ownership, Control, and Use
- Password Policy
- Policy Exceptions
- Responsible Disclosure Policy
- Telecommunications