Policy Compliance Audit Report

Policy: Acceptable Use Policy.pdf

Score: 7.0 / 16

Compliance %: 43.75%

Grade: F

Matched Controls:

ISO - A.5.17
Control: Authentication information. Establish and enforce password and authentication requirements. Users must keep passwords secure, avoid sharing accounts, and follow multi-factor authentication as defined in the Acceptable Use Policy.
- 2. Keep passwords secure and do not share accounts.
- 5. Revealing your account password to others or allowing use of your account by others.
- Authorized users are responsible for the security of their passwords and accounts.

ISO - A.5.18
Control: Access rights. Access rights must be assigned based on roles and reviewed periodically. Unauthorized access or sharing of accounts is prohibited as stated in the Acceptable Use Policy.
- Circumventing user authentication or security of any host, network, or account.
- Please review <Agency Name's> Password Policy for guidance.

ISO - A.5.10
Control: Acceptable use of assets. Define acceptable use of IT assets, including restrictions on unauthorized software, internet misuse, personal email access, and prohibited activities. Monitoring of user activity is permitted as outlined in the Acceptable Use Policy.
- For security and network maintenance purposes, authorized individuals within <Agency Name> may monitor equipment, systems and network traffic at any time, per <Agency Name> Audit Policy>.
- Inappropriate use exposes <Agency Name> to risk including virus attacks, compromises of the network systems and services, and legal issues.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

ISO - A.5.13
Control: Labelling of information. Define and implement labelling requirements for information classification (Confidential, Internal, Public) as described in the Information Security Policy and Acceptable Use Policy.
- For guidance on information classification, see <Agency Name> Information Classification Policy.
- The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or non-confidential, as defined by agency confidentiality guidelines.

ISO - A.8.2.1
Control: Classification of information. Classify information based on sensitivity (e.g., NCIC data) and

enforce encryption and access controls in alignment with the Acceptable Use Policy.
- 3. <Agency Name> security department recommends that any information that a user considers sensitive or vulnerable (etc. residual NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted.
- For guidance on information classification, see <Agency Name> Information Classification Policy.

ISO - A.5.29
Control: Information security during disruption. Define procedures to ensure information security is maintained during disruptions, including business continuity and disaster recovery measures outlined in the Information Security Policy.
- Effecting security breaches or disruptions of network communication.
- For the purpose of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

NIST - AC-2
Control: Users must keep passwords secure and must not share accounts, and administrators must manage user accounts including creation, modification, and removal according to the Acceptable Use Policy.
- Authorized users are responsible for the security of their passwords and accounts.
- 2. Keep passwords secure and do not share accounts.
- 5. Revealing your account password to others or allowing use of your account by others.

NIST - IA-5
Control: Passwords must meet complexity requirements and be kept confidential, with account sharing strictly prohibited, as outlined in the Acceptable Use Policy.
- 5. Revealing your account password to others or allowing use of your account by others.
- Please review <Agency Name's> Password Policy for guidance.
- 2. Keep passwords secure and do not share accounts.

NIST - SC-12
Control: Sensitive data such as NCIC information must be encrypted both in transit and at rest, in accordance with the Acceptable Use Policy.
- 3. <Agency Name> security department recommends that any information that a user considers sensitive or vulnerable (etc. residual NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted.

NIST - SC-28
Control: Sensitive information including NCIC data must be protected through encryption and restricted access in compliance with the Acceptable Use Policy.
- 3. <Agency Name> security department recommends that any information that a user considers sensitive or vulnerable (etc. residual NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted.
- Examples of confidential information include, but are not limited to: NCIC information, state criminal history information, agency personnel data, etc.
- Because of the need to protect <Agency Name's> network, management cannot guarantee the confidentiality of information stored on any network devise belonging to <Agency Name>.

NIST - PL-2

Control: Security policies including acceptable use, access control, and encryption requirements must be documented and enforced as referenced in the Acceptable Use Policy.

- Acceptable Use Policy 1.0 Overview The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to <Agency Name> established culture of openness, trust, and integrity.
- Please review <Agency Name's> Password Policy for guidance.
- 5.0 Enforcement Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data.

CIS - 4.2

Control: Users must keep passwords secure and must not share accounts as required in the Acceptable Use Policy.

- 2. Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- Please review <Agency Name's> Password Policy for guidance.

CIS - 17.1

Control: Users must be informed of security requirements and responsibilities for handling information as outlined in the Acceptable Use Policy.

- Acceptable Use Policy 1.0 Overview The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to <Agency Name> established culture of openness, trust, and integrity.
- It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.
- Inappropriate use exposes <Agency Name> to risk including virus attacks, compromises of the network systems and services, and legal issues.

CIS - 13.4

Control: Sensitive information such as NCIC data must be encrypted and protected from unauthorized access as stated in the Acceptable Use Policy.

- 3. <Agency Name> security department recommends that any information that a user considers sensitive or vulnerable (etc. residual NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted.
- Because of the need to protect <Agency Name's> network, management cannot guarantee the confidentiality of information stored on any network devise belonging to <Agency Name>.
- Examples of confidential information include, but are not limited to: NCIC information, state criminal history information, agency personnel data, etc.

CIS - 5.29

Control: Information security must be maintained during network disruptions or security incidents, in alignment with the Acceptable Use Policy.

- Effecting security breaches or disruptions of network communication.
- For the purpose of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Effective security is a team effort involving the participation and support of every <Agency Name> employee and affiliate who deals with information and/or information systems.

CIS - 8.2.1
Control: Information must be labeled and classified (Confidential, Internal, Public) according to the organization's Information Classification Policy referenced in the Acceptable Use Policy.
- For guidance on information classification, see <Agency Name> Information Classification Policy.
- The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or non-confidential, as defined by agency confidentiality guidelines.
- Acceptable Use Policy 1.0 Overview The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to <Agency Name> established culture of openness, trust, and integrity.

Gaps:

ISO - A.5.17 -> partial
Justification: The policy partially addresses the control. It clearly covers the user's responsibility to keep passwords secure and avoid sharing accounts ('2. Keep passwords secure and do not share accounts.' and '5. Revealing your account password to others or allowing use of your account by others.'). However, the policy completely fails to address the critical requirement regarding multi-factor authentication ('...and follow multi-factor authentication as defined in the Acceptable Use Policy.'). Furthermore, while it addresses user behavior, it does not detail how the organization 'Establishes and enforces password and authentication requirements' in terms of technical specifications (e.g., password complexity, length, lockout policies), focusing solely on user actions.

ISO - A.5.18 -> partial
Justification: The policy partially addresses the control by prohibiting 'circumventing user authentication or security of any host, network, or account,' which directly aligns with the 'unauthorized access' aspect of the control. However, it completely fails to address the critical requirements for 'access rights must be assigned based on roles' and 'reviewed periodically.' While 'sharing of accounts' is strongly implied by 'circumventing user authentication,' it is not explicitly stated as prohibited. The reference to a 'Password Policy' provides no content within this policy itself to meet the control requirements.

ISO - A.5.10 -> partial
Justification: The policy partially addresses the control by explicitly stating that monitoring of equipment, systems, and network traffic is permitted for security and network maintenance purposes. It also defines one specific prohibited activity related to network monitoring/data interception by employees. However, the policy fails to define acceptable use of IT assets broadly, and crucially, it does not include restrictions on unauthorized software, internet misuse, or personal email access, which are explicitly required by the control. The policy mentions 'inappropriate use' but does not elaborate on what constitutes such use beyond the single example provided.

ISO - A.5.13 -> partial
Justification: The policy partially addresses the control by acknowledging information classification and deferring detailed guidance to an '<Agency Name> Information Classification Policy'. This is a common and

acceptable practice for detailed definitions. However, the provided policy snippet itself falls short in several key areas: 1. **Scope of Labelling:** The control requires defining labelling requirements for 'information classification' generally. The policy, however, specifically limits its scope to 'The user interface for information contained on Internet/Intranet/Extranet-related systems,' which is a much narrower scope than general information labelling (e.g., for documents, emails, databases, physical media). 2. **Missing Classification Level:** The control explicitly lists 'Confidential, Internal, Public' as required classification levels. The policy only mentions 'confidential or non-confidential' for user interfaces, and does not explicitly address or define 'Internal' as a distinct classification level within its own stated scope, or explicitly map 'non-confidential' to 'Internal' and 'Public'. While 'non-confidential' might broadly cover 'Internal' and 'Public', the control asks for specific levels to be addressed. 3. **Direct Definition vs. Delegation:** While delegating to another policy is fine for detailed definitions, the control asks the policy to 'Define and implement labelling requirements'. The provided snippet mostly delegates without providing sufficient detail or explicitly stating *how* labelling is implemented beyond the UI classification for specific systems. It doesn't elaborate on the 'requirements' themselves. Therefore, while the policy identifies classification and points to a source for detailed guidance, it does not fully define or implement comprehensive labelling requirements for all information, nor does it explicitly address all required classification levels within its directly stated scope.

ISO - A.8.2.1 -> partial
Justification: The policy partially addresses the control, but significant gaps exist: 1. **Classification:** The policy refers to an external 'Information Classification Policy' for guidance, indicating that this policy snippet does not define or enforce the classification process itself. Furthermore, it implies user discretion ('information that a user considers sensitive') for identifying sensitive data, which may contradict a formal, agency-wide classification scheme required by the control. 2. **Enforce Encryption:** The policy states that encryption is 'recommended' for sensitive information. The control, however, explicitly requires *enforcement* of encryption. A recommendation is insufficient to meet an enforcement requirement. 3. **Access Controls:** The policy makes no mention of enforcing access controls whatsoever. 4. **Alignment with AUP:** The policy does not mention alignment with an Acceptable Use Policy. 5. **Sensitive Data Examples:** The policy correctly identifies examples of sensitive data (e.g., NCIC, CJIS information), aligning with the control's examples of information requiring protection.

ISO - A.5.29 -> none
Justification: The control requires defining procedures to ensure information security is maintained *during* disruptions, explicitly including business continuity and disaster recovery measures. The provided policy snippet only defines what constitutes a 'disruption' for the purpose of the policy. It does not outline any procedures, measures, or guidelines for maintaining information security, business continuity, or disaster recovery when such disruptions occur. It defines the malicious act, but does not address the organizational response to it.

NIST - AC-2 -> partial
Justification: The policy adequately addresses the user's responsibility to keep passwords secure and not share accounts, as covered in points 1, 2, and 5. However, the policy completely fails to address the second part of the control, which dictates that 'administrators must manage user accounts including creation, modification, and removal according to the Acceptable Use Policy'. This critical

administrative function and its associated lifecycle management are not mentioned in the provided policy excerpts.

NIST - IA-5 -> partial
Justification: The policy partially addresses the control. It explicitly covers the requirements for keeping passwords confidential ('Keep passwords secure') and strictly prohibits account sharing ('Revealing your account password to others or allowing use of your account by others', 'do not share accounts'). However, the policy does not define or outline the password complexity requirements itself; instead, it defers this specific detail to an external '<Agency Name's> Password Policy'. Therefore, this policy snippet does not fully encompass all aspects of the control.

NIST - SC-12 -> none
Justification: The policy fails to address the control adequately on several critical points: 1. **Mandatory vs. Recommended:** The control states that sensitive data *'must be encrypted'*, indicating a mandatory requirement. The policy, however, only *'recommends'* encryption, making it optional and not enforceable. 2. **Scope and Definition of Sensitive Data:** The control specifies 'Sensitive data such as NCIC information'. The policy relies on what 'a user considers sensitive or vulnerable,' which introduces subjective interpretation and does not ensure that all NCIC information (which is inherently sensitive) is consistently encrypted. 3. **States of Data:** The control explicitly requires encryption 'both in transit and at rest'. The policy makes no mention of these specific states, leaving a significant gap in coverage for data movement and storage. Due to these fundamental discrepancies, the policy does not ensure compliance with the control.

NIST - SC-28 -> partial
Justification: The policy partially addresses the control but contains significant weaknesses and omissions. While the policy correctly identifies NCIC information as sensitive and recommends encryption as a protection method, it falls short in several critical areas: 1. **Mandatory vs. Recommended:** The control states that sensitive information *'must be protected through encryption'*, using strong, mandatory language. In contrast, the policy states that the security department *'recommends'* encryption. A recommendation does not fulfill a mandatory requirement. 2. **Restricted Access:** The control explicitly requires protection through *'restricted access'*. The policy makes no mention of restricted access whatsoever. 3. **Acceptable Use Policy (AUP) Compliance:** The control requires protection *'in compliance with the Acceptable Use Policy'*. The policy does not mention compliance with an AUP. 4. **Contradictory Statement:** The policy includes a highly problematic statement: *'management cannot guarantee the confidentiality of information stored on any network devise belonging to <Agency Name>'*. This directly contradicts the core intent of the control, which is to ensure sensitive information *is* protected and its confidentiality maintained. A policy stating that confidentiality cannot be guaranteed is in direct opposition to a control requiring protection of sensitive information. In summary, while the policy identifies the data and one protection method, its non-mandatory language, significant omissions (restricted access, AUP), and a statement disclaiming the ability to guarantee confidentiality render it largely insufficient to meet the control's requirements.

NIST - PL-2 -> partial
Justification: The policy effectively functions as the documented Acceptable Use Policy and includes a dedicated 'Enforcement' section (5.0), addressing the documentation and enforcement aspects for itself. It also references a 'Password Policy,' which is a component of access control, thereby partially

addressing the requirement for documenting access control. However, the policy does not explicitly address the comprehensive documentation or enforcement of broader 'access control requirements' beyond passwords, nor does it make any mention of 'encryption requirements' being documented or enforced, as specified by the control. The control specifically requires that these types of policies *including* encryption must be documented and enforced *as referenced in the AUP*, which is not fully met for all specified policy types.

CIS - 4.2 -> full
Justification: The policy directly addresses both key requirements of the control by stating "Keep passwords secure and do not share accounts." It further reinforces this by clarifying that "Authorized users are responsible for the security of their passwords and accounts." This clearly covers the control's demands for users to secure passwords and not share accounts.

CIS - 17.1 -> partial
Justification: The policy implicitly addresses the existence of guidelines and user responsibility ('It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly'). However, it falls short of fully addressing the control because: 1. It does not specify *how* users are informed of these requirements and responsibilities (e.g., mandatory training, email dissemination, policy acknowledgment). It places the onus on the user to 'know' rather than the agency to 'inform.' 2. While it mentions 'guidelines' and 'responsibilities,' it does not *outline* any specific security requirements or responsibilities for handling information. It only broadly refers to 'inappropriate use' and associated risks, without detailing what 'appropriate use' or 'secure handling of information' entails. The control explicitly states 'as outlined in the Acceptable Use Policy,' implying these details should be present within the policy itself, which they are not in this provided excerpt.

CIS - 13.4 -> none
Justification: The control mandates that sensitive information 'must be encrypted' and 'protected from unauthorized access'. The policy significantly deviates from these requirements: 1. **Encryption Mandate:** The policy states that the security department 'recommends' encryption, which is advisory and not a mandatory requirement as stipulated by the control ('must be encrypted'). 2. **Protection/Confidentiality Guarantee:** The policy explicitly states that management 'cannot guarantee the confidentiality of information', which directly contradicts the control's requirement for information to be 'protected from unauthorized access'. While the policy correctly identifies NCIC information as sensitive, its failure to mandate encryption and its explicit statement that confidentiality cannot be guaranteed means it does not address the core requirements of the control.

CIS - 5.29 -> partial
Justification: The policy defines what constitutes a 'disruption' and prohibits actions that cause security breaches or disruptions, which aligns with the 'Acceptable Use Policy' aspect of the control by defining unacceptable behavior. It also includes a general statement about security being a 'team effort'. However, the control specifically requires that 'Information security must be maintained during network disruptions or security incidents'. The provided policy text does not articulate *how* information security is to be maintained during such events. It lacks details on incident response procedures, security measures, roles, or responsibilities for ensuring security posture and data integrity while a disruption or incident is ongoing.

CIS - 8.2.1 -> partial
Justification: The policy partially addresses the control. It successfully references the <Agency Name> Information Classification Policy, and this reference appears within the same document as the 'Acceptable Use Policy 1.0 Overview,' thus fulfilling the requirement for the AUP to reference it. It also indicates that information should be classified. However, the policy text explicitly defines classification for user interfaces on Internet/Intranet/Extranet-related systems as 'confidential or non-confidential.' This does not fully align with the more granular 'Confidential, Internal, Public' categories specifically mandated by the control, failing to explicitly distinguish between 'Internal' and 'Public' information.

Remediation Suggestions:

ISO - A.5.17
Suggestion: The policy should be updated to explicitly state the organization's role in establishing authentication requirements and to incorporate the multi-factor authentication (MFA) mandate. **Recommended Policy Additions/Modifications:** 1. **Add a new introductory clause (or integrate into an appropriate existing section):** "The organization shall establish and enforce comprehensive password and authentication requirements for all user accounts and systems. These requirements, including specifics on password complexity, length, history, and account lockout procedures, will be further detailed in the Acceptable Use Policy (AUP) or a dedicated Password Standard." 2. **Modify or add to the user responsibilities section (e.g., expand on point 2 or create a new point):** "Users must keep passwords secure, avoid sharing accounts, and strictly adhere to all established password and authentication requirements. Where mandated, users are also required to utilize multi-factor authentication (MFA) as defined in the Acceptable Use Policy (AUP). Revealing your account password to others or allowing the use of your account by others is strictly prohibited. Authorized users are responsible for the security of their passwords and accounts, and for compliance with all authentication protocols." **Justification:** * **Organizational Responsibility:** The current policy focuses solely on user responsibility. The control explicitly states the organization's duty to "Establish and enforce password and authentication requirements." The suggested addition addresses this by defining the organization's role. * **Multi-Factor Authentication (MFA):** The control explicitly mentions "follow multi-factor authentication as defined in the Acceptable Use Policy." The current policy makes no mention of MFA, which is a critical security measure. The suggested addition directly incorporates this requirement. * **Specificity of Requirements:** While the control mentions "password and authentication requirements," the policy is vague. By referencing the AUP or a dedicated standard for specifics (complexity, length, etc.), the policy becomes more robust and aligns with the control's implication of defined requirements.

ISO - A.5.18
Suggestion: The policy should be updated to explicitly prohibit 'sharing of accounts' as stated in the control, either by adding this prohibition directly or by clearly referencing the 'Acceptable Use Policy' where this is detailed. Additionally, while 'circumventing user authentication' covers a method of unauthorized access, the policy could also broadly state the prohibition against 'unauthorized access' in line with the control, again, by direct inclusion or by a clear cross-reference to the 'Acceptable Use Policy'. This ensures that all elements of the control's stated prohibitions are explicitly addressed or clearly linked within the policy structure, providing comprehensive guidance

to users and aligning policy enforcement with control requirements.

ISO - A.5.10
Suggestion: Revise the Acceptable Use Policy (AUP) to explicitly state that user activity on agency IT assets (e.g., internet usage, email, software installations, file access) is subject to monitoring. The AUP should clearly define the purpose of such monitoring (e.g., security, compliance, network maintenance, policy enforcement) and inform users that, by utilizing agency resources, they acknowledge and consent to this monitoring. While the policy references an 'Audit Policy,' ensure that either the AUP itself or the referenced Audit Policy comprehensively details how user activity monitoring is conducted to enforce acceptable use, thereby closing the gap identified in the control.

ISO - A.5.13
Suggestion: The policy should be updated to explicitly define and differentiate between 'Confidential', 'Internal', and 'Public' information classifications, including clear criteria, examples, and associated handling requirements for each. If this detailed definition resides in a separate 'Information Classification Policy', the current Information Security Policy and Acceptable Use Policy must prominently and consistently cross-reference it. Additionally, the policy needs to clarify how 'non-confidential' information, as mentioned for user interfaces, maps directly to the 'Internal' and 'Public' classifications to ensure consistent understanding and application of the three-tier labelling scheme mandated by the control across all information types and systems.

ISO - A.8.2.1
Suggestion: Revise Policy Section 3 to replace 'recommends' with mandatory language (e.g., 'requires' or 'shall ensure') and remove the phrase 'that a user considers sensitive or vulnerable.' The revised policy should clearly state that all information classified as sensitive (referencing the Information Classification Policy) must be encrypted and subject to appropriate access controls. This ensures the policy reflects the control's directive to enforce protection based on objective classification, rather than subjective user discretion or mere recommendation.

ISO - A.5.29
Suggestion: The current 'Policy' provides a narrow definition of 'disruption,' limited primarily to malicious network communication activities. In contrast, the 'Control' requires the establishment of procedures to maintain information security during a much broader scope of disruptions, including business continuity and disaster recovery measures that encompass events like natural disasters, system failures, power outages, and diverse cyber incidents. **Remediation:** 1. **Expand 'Disruption' Definition:** Update the existing policy, or create a new overarching 'Information Security Disruption & Resilience Policy,' to significantly broaden the definition of 'disruption.' This expanded definition must comprehensively cover all types of events that could potentially impact information security and business operations, aligning with the scope required for robust business continuity and disaster recovery planning. 2. **Incorporate BC/DR Procedures:** Within this revised or new policy, explicitly outline or directly reference the detailed procedures, responsibilities, and measures for maintaining information security during *all* identified types of disruptions. This must include specific guidance on incident response, business continuity, and disaster recovery processes to directly address the control's requirement for defined procedures.

NIST - AC-2

Suggestion: The primary gap between the control and the policy is the policy's complete omission of administrator responsibilities regarding user account management (creation, modification, removal). The policy currently focuses solely on user responsibilities. **Remediation:** 1. **Expand Policy to Include Administrator Responsibilities:** Add a new section or clause to the policy that explicitly outlines the administrator's role in managing user accounts. This section should mirror the control's requirement for administrators to manage account lifecycles (creation, modification, and removal) in accordance with the Acceptable Use Policy (AUP). * *Example Policy Text:* "Administrators are responsible for the lifecycle management of user accounts, including their creation, modification, and removal, in strict adherence to the Acceptable Use Policy." 2. **Clarify Prohibited Actions:** While policy point 5 hints at it, it's not a complete sentence and lacks the directness of a clear prohibition. Rephrase or integrate it more formally as a prohibited action. * *Example Policy Text (Refinement of existing point):* "Sharing your account password with others or allowing unauthorized use of your account by others is strictly prohibited and constitutes a violation of this policy."

NIST - IA-5
Suggestion: To fully align the policy with the control's 'strictly prohibited' language and enforce the gravity of non-compliance, the policy should be updated to: 1. **Explicitly State Prohibitions:** Rephrase or add language that clearly labels revealing passwords, allowing account use by others, and account sharing as 'strictly prohibited' actions, mirroring the control's wording. 2. **Outline Consequences:** Include a clear statement outlining the disciplinary actions or consequences for violating these rules, referencing the Acceptable Use Policy (AUP) or other relevant HR/disciplinary frameworks. This directly reinforces the 'strictly prohibited' aspect and ensures users understand the impact of non-compliance.

NIST - SC-12
Suggestion: The primary gap lies in the policy's advisory language ('recommends') versus the control's mandatory language ('must be encrypted'), and the subjective definition of 'sensitive' data in the policy compared to the control's specific examples. **Remediation:** Amend Policy 3 to explicitly state that NCIC information and other designated sensitive data (e.g., CJIS-related information) *must* be encrypted, aligning with the control's mandatory requirement. The policy should also clarify that this mandatory encryption applies 'both in transit and at rest.' Furthermore, the policy should define or provide specific categories/examples of data that fall under the mandatory 'sensitive data' classification, rather than solely relying on user discretion, while still encouraging users to encrypt any other information they deem sensitive.

NIST - SC-28
Suggestion: The policy needs to be revised to align with the mandatory nature of the control. Specifically: 1. **Change 'Recommends' to 'Requires/Mandates':** The policy currently 'recommends' encryption for sensitive data based on user discretion. The control states sensitive information 'MUST be protected through encryption'. The policy must be updated to clearly state that encryption is *required* for all specified sensitive information (e.g., NCIC data, state criminal history, personnel data) regardless of individual user assessment. 2. **Define Mandatory Protection Methods:** The policy should explicitly detail the *mandatory* methods for encryption and restricted access for all identified sensitive data types, moving beyond just a recommendation. This includes specifying approved encryption standards/tools and defining how restricted access (e.g., 'need-to-know' basis,

access control lists, secure storage locations) is to be implemented. 3. **Address the Disclaimer's Contradiction:** The statement 'management cannot guarantee the confidentiality of information stored on any network devise belonging to <Agency Name>' directly contradicts the control's mandate that sensitive information 'MUST be protected'. This section should be rephrased or removed. Instead, the policy should articulate the *joint responsibility* (agency providing tools/guidelines, users adhering to requirements) for maintaining confidentiality, emphasizing that adherence to the mandated controls *is* the mechanism by which confidentiality is achieved/maintained to the best extent possible. 4. **Include 'Restricted Access' Mandate:** While the policy mentions encryption, it doesn't explicitly mandate 'restricted access' as the control does. The policy should include clear requirements for restricting access to sensitive information.

NIST - PL-2
Suggestion: Revise the Acceptable Use Policy (AUP) to explicitly incorporate or reference comprehensive sections on 'Access Control' and 'Encryption Requirements,' detailing the specific policies and procedures for each. Furthermore, expand the 'Enforcement' section of the AUP beyond just listing violations to clearly define the enforcement process, including reporting mechanisms, investigation procedures, and potential disciplinary actions for non-compliance, ensuring it aligns with documented enforcement guidelines.

CIS - 17.1
Suggestion: The Acceptable Use Policy needs to be augmented to describe the *mechanisms* by which users are actively informed of its contents, rather than solely placing the onus on the user to know. The current policy states it's the user's responsibility to know, but doesn't outline how the agency fulfills its obligation to *inform* them, as required by the control. Proposed additions to the policy or supporting procedures could include: 1. **Mandatory Training Integration:** Specify that all users must complete initial and recurring security awareness training that explicitly covers the Acceptable Use Policy and its implications. This ensures the 'informed' requirement of the control is met. 2. **Attestation/Acknowledgement Process:** Implement a formal process where users are required to acknowledge (e.g., via digital signature, click-through agreement) that they have read, understood, and agree to abide by the Acceptable Use Policy. This acknowledgment should be required upon initial system access, annually thereafter, and/or upon significant policy updates. 3. **Onboarding Requirement:** Make the review and acknowledgment of the Acceptable Use Policy a mandatory step in the new employee/user onboarding process. 4. **Communication Strategy:** Outline a strategy for periodic communication (e.g., email reminders, intranet posts, pop-up notifications) reinforcing AUP requirements and responsibilities, especially when new risks or changes emerge.

CIS - 13.4
Suggestion: The policy should be revised to mandate encryption for all identified sensitive information (e.g., NCIC data, state criminal history information, agency personnel data) rather than merely recommending it or leaving it to user discretion. The phrase 'recommends that any information that a user considers sensitive or vulnerable... be encrypted' should be changed to 'requires that all sensitive information, including but not limited to NCIC information, state criminal history information, and agency personnel data, be encrypted and protected from unauthorized access.' Additionally, the statement 'management cannot guarantee the confidentiality of information stored on any network devise' directly contradicts the control's 'must be encrypted and protected from unauthorized access' and should be revised or removed to reflect the agency's commitment to actively

securing sensitive data.

CIS - 5.29

Suggestion: Augment the policy to include explicit requirements for incident response and business continuity, detailing the procedures, roles, and responsibilities for *maintaining* information security during network disruptions and security incidents. This would bridge the gap between defining and prohibiting disruptions, and outlining the active organizational measures taken to secure systems during such events as required by the control.

CIS - 8.2.1

Suggestion: Revise the Policy's specific guidance for 'Internet/Intranet/Extranet-related systems' to explicitly align with the three classification levels mandated by the Control: 'Confidential, Internal, and Public.' The current policy's 'confidential or non-confidential' creates a discrepancy. The policy should either replace 'non-confidential' with 'Internal' and 'Public' as distinct options, or clearly define how 'non-confidential' encompasses and differentiates between 'Internal' and 'Public' information, ensuring consistency with the organization's overarching 'Information Classification Policy' referenced by both documents.