TO: John Kasket, Chief Information Security Officer

FROM: Richie Nguyen, Information Security Analyst

DATE: November 16, 2025

RE: Updated ACME Corporation 2025 Policies and Justifications

Memorandum

This memorandum summarizes the core reasons for ACME Corporation's updated policies for November 2025. The previous 2020 policies do not reflect current threats or regulatory expectations. The updated policy demonstrates clear, mandatory standards in cybersecurity, identity management, vulnerability patching, incident response, and data privacy. These changes are necessary to protect confidentiality, integrity, availability and align ACME's security with modern best practices.

Need for Policy Modernization

The threat landscape has evolved significantly in the last five years, and attackers now routinely exploit weak, unpatched systems. Along with the inconsistent incident reporting processes of the past, the attack surface of the company has expanded significantly. The existing policy framework relied heavily on optional controls, which led to inconsistent practices across all departments. This has led to the need for a revised policy that practices mandatory standards deemed essential for accountability and availability. With clearer requirements, employees are expected to better understand the expectations and verification pipelines needed for secure development and continued operation.

Cybersecurity

The core policy was redesigned with standardization and clear roles in mind. By following principles such as Least Privilege and Zero Trust, the organization will establish

another layer of security with a clear structure to be able to better address modern threats. Without a clear framework, communication between departments stays inconsistent, which creates gaps that attackers could exploit. The new policy establishes consistency across the entire organization and ensures accountability at all levels.

Identity and Access Management

The previous Password Policy was not broad enough to cover modern standards and Role-based access that the company needs to adopt. With credential compromise being a cause of data breaches, the new policy implements multi-factor authentication, modern password standards, and immediate deprovisioning of accounts upon termination. In compliance with GDPR and CCPA, these changes directly reduce the risk of unauthorized access and the lack of information on how accounts must be removed in the previous policy.

Data Privacy and Acceptable Use

Updated from the previous Data Privacy Policy, this new policy aims to have clearer classifications to reduce delays and inconsistent handling of potential threats. With structured classification and a clear Acceptable Use policy, any employee expectations on data use and privacy are managed to ensure that sensitive information receives appropriate protections.

Incident Response

This new policy introduces several incident classifications and incident phases to define response timelines as well as the responsibilities of employees during times of crisis. Without a well-defined framework for incident remediation, the lack of containment could cause compromised systems and inconsistent handling of potential threats.

Vulnerability and Patch Management

A dedicated policy is necessary to prevent the continued use of outdated systems and to further effective vulnerability remediation. The clear requirements for scanning and prioritization ensure that ACME closes security gaps promptly. Along with established asset ownership and clear patch timelines, these changes reduce avoidable risk to the system.

Timeline

The implementation of these updated changes will occur in three phases over a six-month period. The first phase focuses on foundational changes such as clearer communication guidelines, mandatory security awareness training, enforcement of password standards and MFA, and lastly, the launch of the incident reporting system. This ensures that employees understand their roles and responsibilities in a timely manner, and immediate controls are put in place. The second two-month phase will focus on RBAC, automatic provisioning and deprovisioning, vulnerability scanning tools, and defining patch management processes throughout the organization. Lastly, integrating consistent compliance monitoring and conducting annual policy reviews will be the final components of the policy implementations.

Conclusion

The November 2025 Policies are necessary to update and modernize ACME's approach to security and address relevant, current threats. The revised policies provide clearer standards for identity management, vulnerability remediation, incident handling, and data privacy across multiple departments. Together, these changes create a more resilient security environment capable of handling emerging threats to protect ACME's assets, maintaining customer and employee trust, and supporting long-term stability.