Creating and Enforcing Security Policies in Organisations.

Created by Samsudeen Olapade.

1. Introduction

Security policies are the backbone of an organisation's cybersecurity framework. They provide clear guidelines for how employees, contractors, and third parties should handle information systems, networks, and data. Using industry-recognized standards such as the SANS Institute policy templates, organizations can ensure their security practices are consistent, enforceable, and aligned with best practices.

This documentation provides a step-by-step guide on how to create and enforce organizational security policies, focusing on:
- Acceptable Use Policy (AUP)
- Privacy Policy
- Password Policy
- Database Security Policy
- Web Application Security Policy

2. Framework for Developing Policies

1. Reference Standards: Use established frameworks such as SANS.org security policy templates, NIST guidelines, and ISO/IEC 27001.
2. Assess Organisational Needs: Conduct risk assessments to identify threats relevant to your environment (e.g., insider threats, external attackers, compliance obligations).
3. Draft the Policy: Ensure policies clearly state the purpose, scope, responsibilities, and enforcement measures.
4. Review and Approve: Circulate drafts to management, legal, and technical teams for validation.
5. Communicate and Train: Provide training sessions and accessible documentation so employees understand their responsibilities.
6. Enforce: Implement technical controls (firewalls, authentication systems, logging) and administrative controls (audits, monitoring, disciplinary measures).
7. Review and Update: Policies must be reviewed periodically (e.g., annually) or after major organizational or regulatory changes.

3. Core Security Policies

3.1 Acceptable Use Policy (AUP)

Purpose: Define how employees can use company IT assets (networks, devices, email, internet).

Creation Steps: - Identify acceptable and unacceptable activities (e.g., business vs. personal use).
- Align with compliance requirements (e.g., GDPR, HIPAA).
- Reference SANS AUP template for standard clauses.

Enforcement: - Monitor usage through logging and alerts.
- Use disciplinary actions (warnings, suspension) for violations.
- Include mandatory employee acknowledgment forms.

3.2 Privacy Policy

Purpose: Protect personal and sensitive information handled by the organization.

Creation Steps: - Define categories of data collected (e.g., customer PII, employee HR data).
- State how data is stored, processed, shared, and deleted.
- Align with data protection regulations (GDPR, CCPA, local laws).

Enforcement: - Implement access controls and encryption.
- Audit handling of personal data.
- Conduct annual privacy impact assessments.

3.3 Password Policy

Purpose: Ensure strong authentication and reduce risks of credential compromise.

Creation Steps: - Define minimum requirements (length, complexity, expiry).
- Encourage use of password managers and MFA (multi-factor authentication).
- Reference SANS Password Policy template for technical best practices.

Enforcement: - Configure systems to enforce password rules.
- Monitor for password reuse or breaches.
- Lock accounts after repeated failed login attempts.

3.4 Database Security Policy

Purpose: Safeguard sensitive organizational data stored in databases.

Creation Steps: - Define authorized access roles and permissions.
- Require encryption for data at rest and in transit.
- Establish backup and recovery protocols.

Enforcement: - Use database activity monitoring (DAM) tools.
- Conduct periodic vulnerability assessments.
- Apply least privilege and regular access reviews.

3.5 Web Application Security Policy

Purpose: Secure organizational web applications against common threats.

Creation Steps: - Follow OWASP Top 10 as baseline security requirements.
- Require secure coding practices and regular code reviews.
- Enforce patch management for web servers and applications.

Enforcement: - Implement Web Application Firewalls (WAFs).
- Perform penetration testing and vulnerability scans.
- Establish incident response procedures for web app breaches.

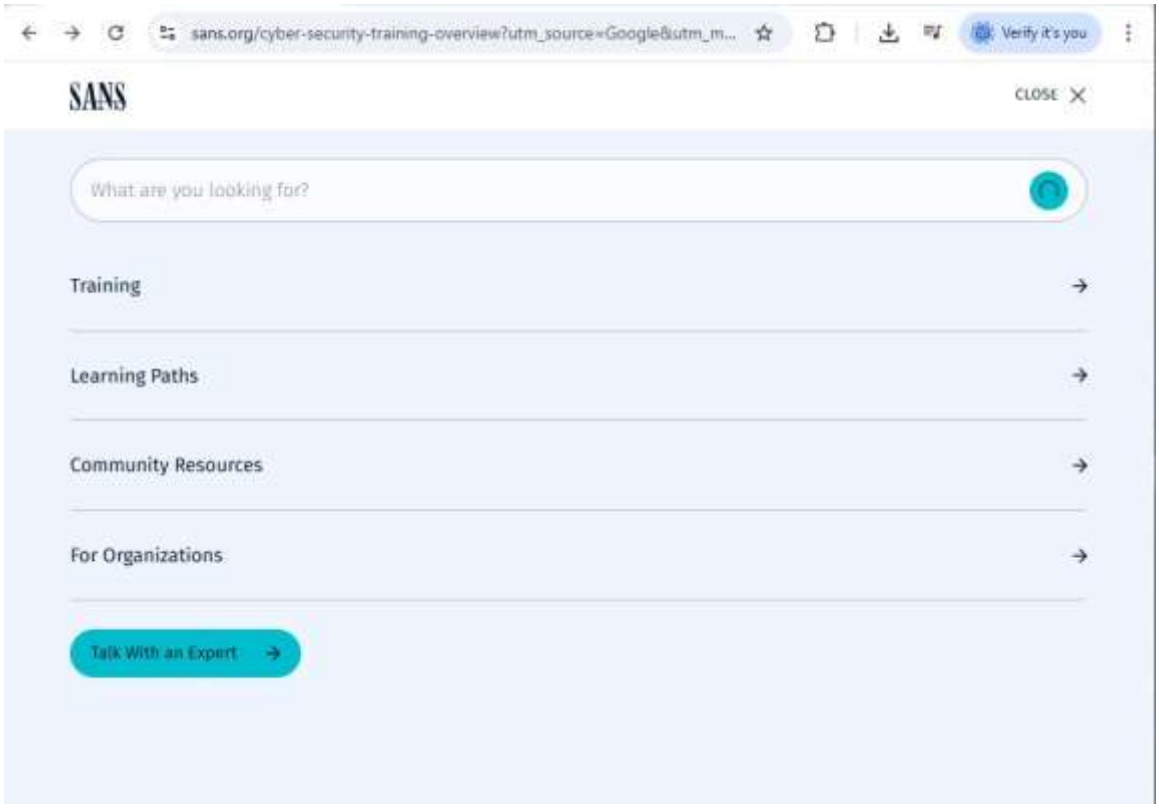
4. Policy Enforcement Strategies

To ensure compliance, organizations must go beyond policy creation. Key enforcement methods include:
- Technical Controls: Firewalls, endpoint protection, MFA, access logs, SIEM monitoring.
- Administrative Controls: Regular training, policy acknowledgment, disciplinary measures.
- Audits and Reviews: Annual reviews of policy effectiveness and compliance checks.
- Incident Response Integration: Policies must align with the organization's incident response plan.

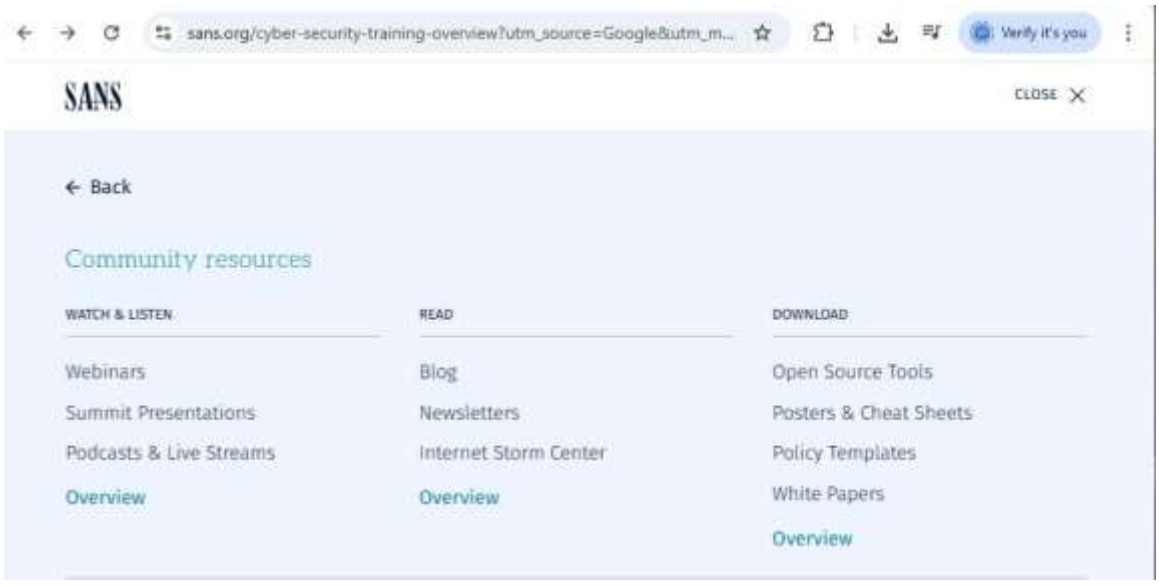
5. Aligning with SANS.org Policies

SANS Institute provides policy templates that organizations can adapt to their environment. To follow SANS policies effectively:
- Map organizational policies against SANS templates (to avoid gaps).
- Adopt SANS baseline requirements (e.g., for passwords, AUPs, data security).
- Customize policies to reflect company culture, industry requirements, and regulatory obligations.
- Use SANS training resources to strengthen employee awareness and compliance.

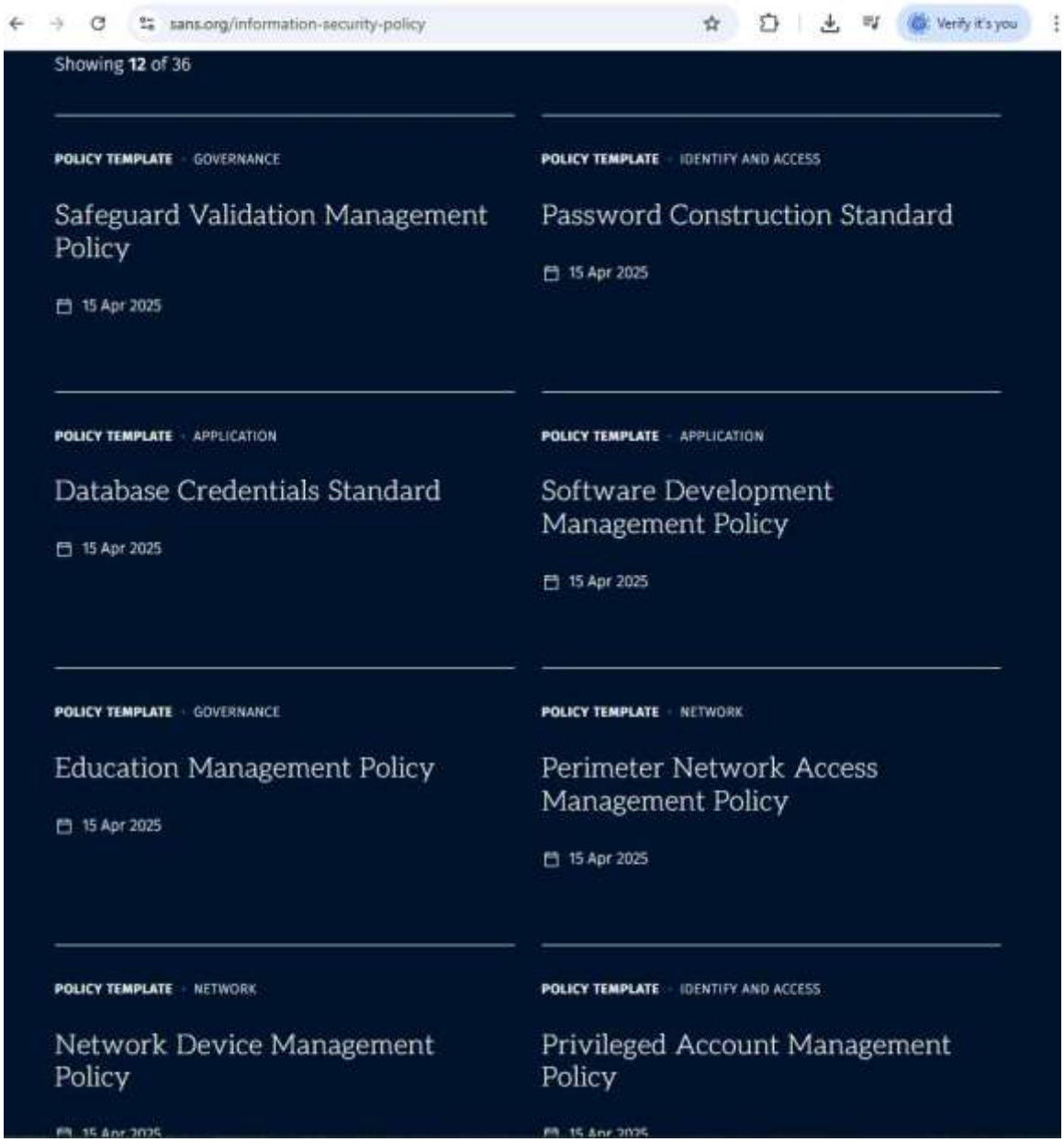
How to Get Policies from SANS.org:
1. Visit https://www.sans.org
2. Click on Community Resources.

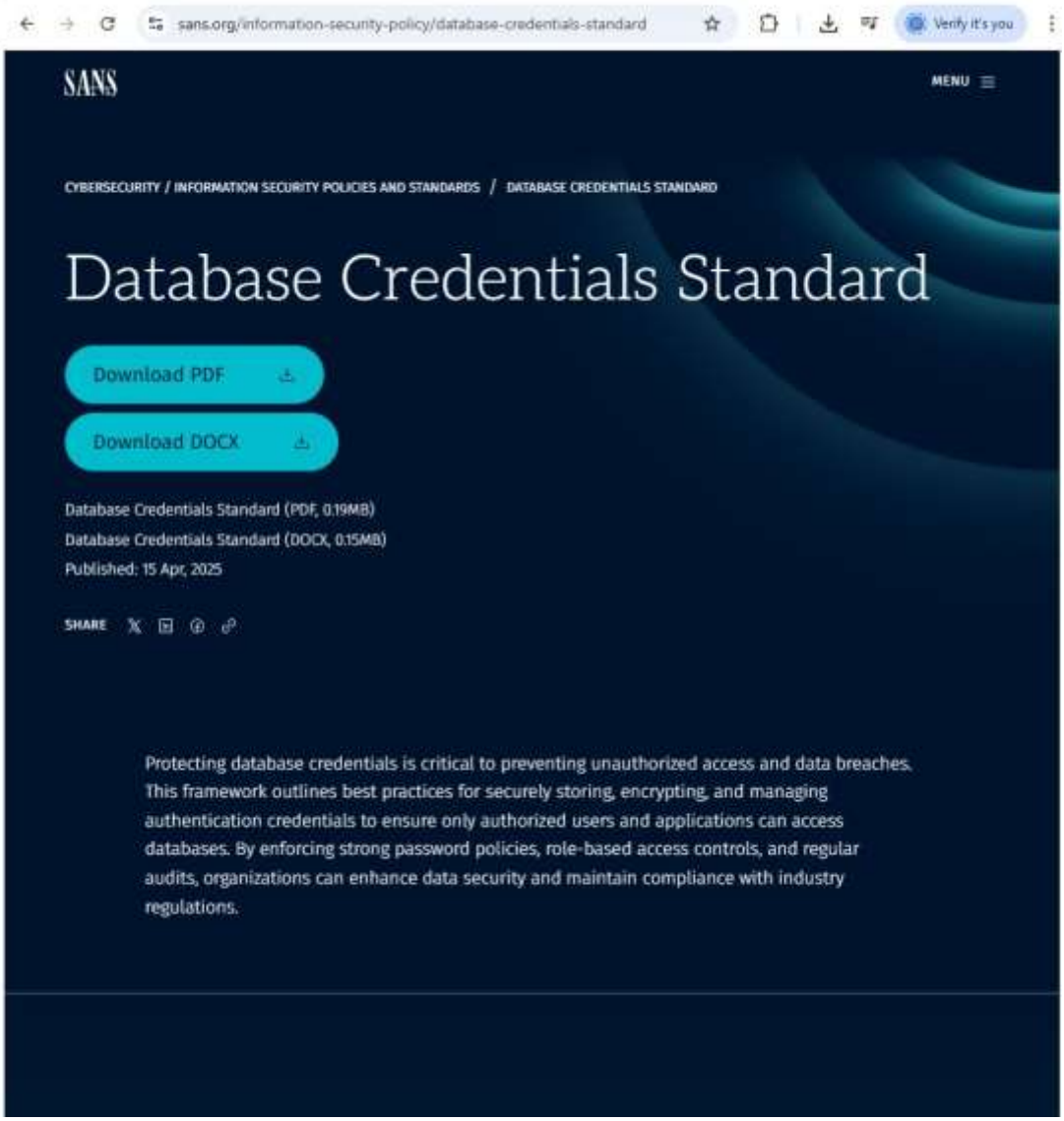


3. Click on Policy Templates

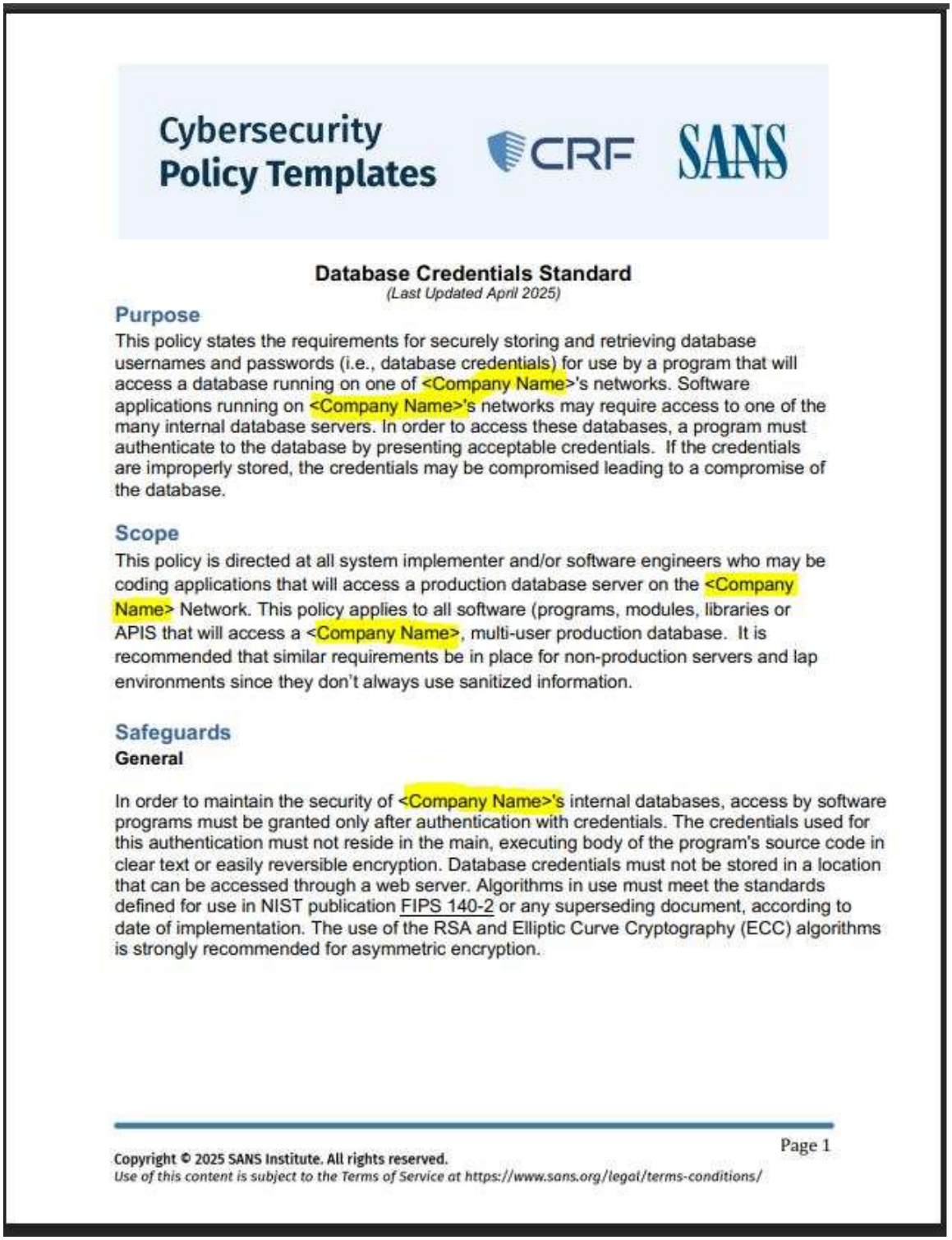


4. Scroll down and download the relevant template **(e.g. Database Credentials Standard (this is used for the purpose of this documentation.)**).


sans.org/information-security-policy
Verify it's you
Showing 12 of 36
POLICY TEMPLATE · GOVERNANCE
Safeguard Validation Management Policy
15 Apr 2025
POLICY TEMPLATE · IDENTIFY AND ACCESS
Password Construction Standard
15 Apr 2025
POLICY TEMPLATE · APPLICATION
Database Credentials Standard
15 Apr 2025
POLICY TEMPLATE · APPLICATION
Software Development Management Policy
15 Apr 2025
POLICY TEMPLATE · GOVERNANCE
Education Management Policy
15 Apr 2025
POLICY TEMPLATE · NETWORK
Perimeter Network Access Management Policy
15 Apr 2025
POLICY TEMPLATE · NETWORK
Network Device Management Policy
POLICY TEMPLATE · IDENTIFY AND ACCESS
Privileged Account Management Policy


sans.org/information-security-policy/database-credentials-standard
Verify it's you
SANS
MENU
CYBERSECURITY / INFORMATION SECURITY POLICIES AND STANDARDS / DATABASE CREDENTIALS STANDARD
Database Credentials Standard
Download PDF
Download DOCX
Database Credentials Standard (PDF, 0.19MB)
Database Credentials Standard (DOCX, 0.15MB)
Published: 15 Apr, 2025
SHARE
Protecting database credentials is critical to preventing unauthorized access and data breaches. This framework outlines best practices for securely storing, encrypting, and managing authentication credentials to ensure only authorized users and applications can access databases. By enforcing strong password policies, role-based access controls, and regular audits, organizations can enhance data security and maintain compliance with industry regulations.

5. Edit it to suit your company requirement. (**for the sake of this documentation, NymousTechnologies is used as the organisation's name**.).



Cybersecurity Policy Templates

CRF SANS

Database Credentials Standard

(Last Updated April 2025)

Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of <Company Name>'s networks. Software applications running on <Company Name>'s networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

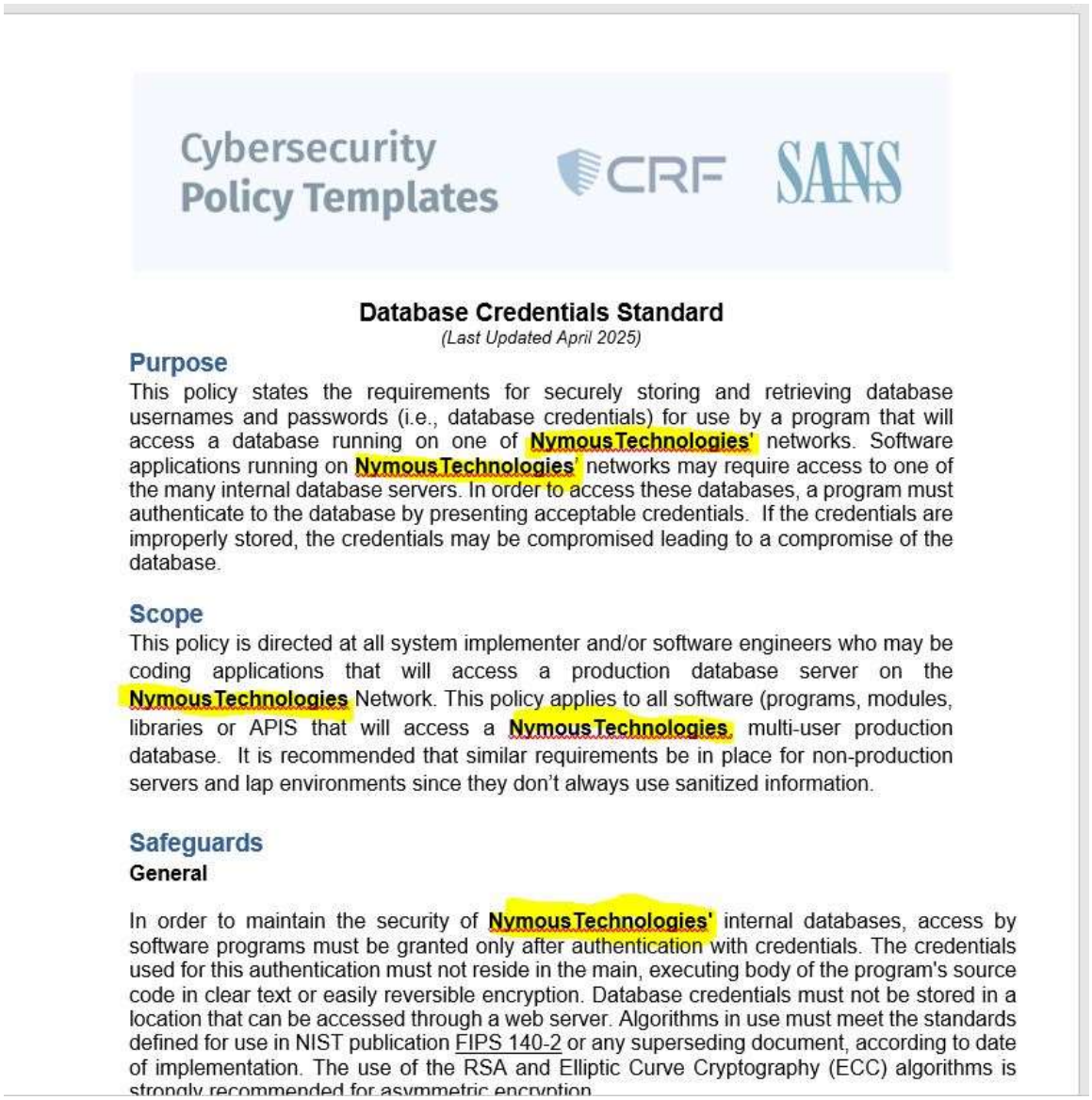
Scope

This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the <Company Name> Network. This policy applies to all software (programs, modules, libraries or APIS that will access a <Company Name>, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they don't always use sanitized information.

Safeguards

General

In order to maintain the security of <Company Name>'s internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text or easily reversible encryption. Database credentials must not be stored in a location that can be accessed through a web server. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.



Cybersecurity Policy Templates

CRF SANS

Database Credentials Standard

(Last Updated April 2025)

Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of NymousTechnologies' networks. Software applications running on NymousTechnologies' networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

Scope

This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the NymousTechnologies Network. This policy applies to all software (programs, modules, libraries or APIS that will access a NymousTechnologies multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they don't always use sanitized information.

Safeguards

General

In order to maintain the security of NymousTechnologies' internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text or easily reversible encryption. Database credentials must not be stored in a location that can be accessed through a web server. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption

6. Conclusion

Creating and enforcing effective security policies requires a structured approach guided by industry standards. By leveraging SANS Institute policy templates, organizations can establish clear, enforceable rules across Acceptable Use, Privacy, Password, Database, and Web Application domains. Enforcement through training, monitoring, audits, and technical controls ensures that policies are not only documented but actively practiced, reducing organizational risk and ensuring compliance.