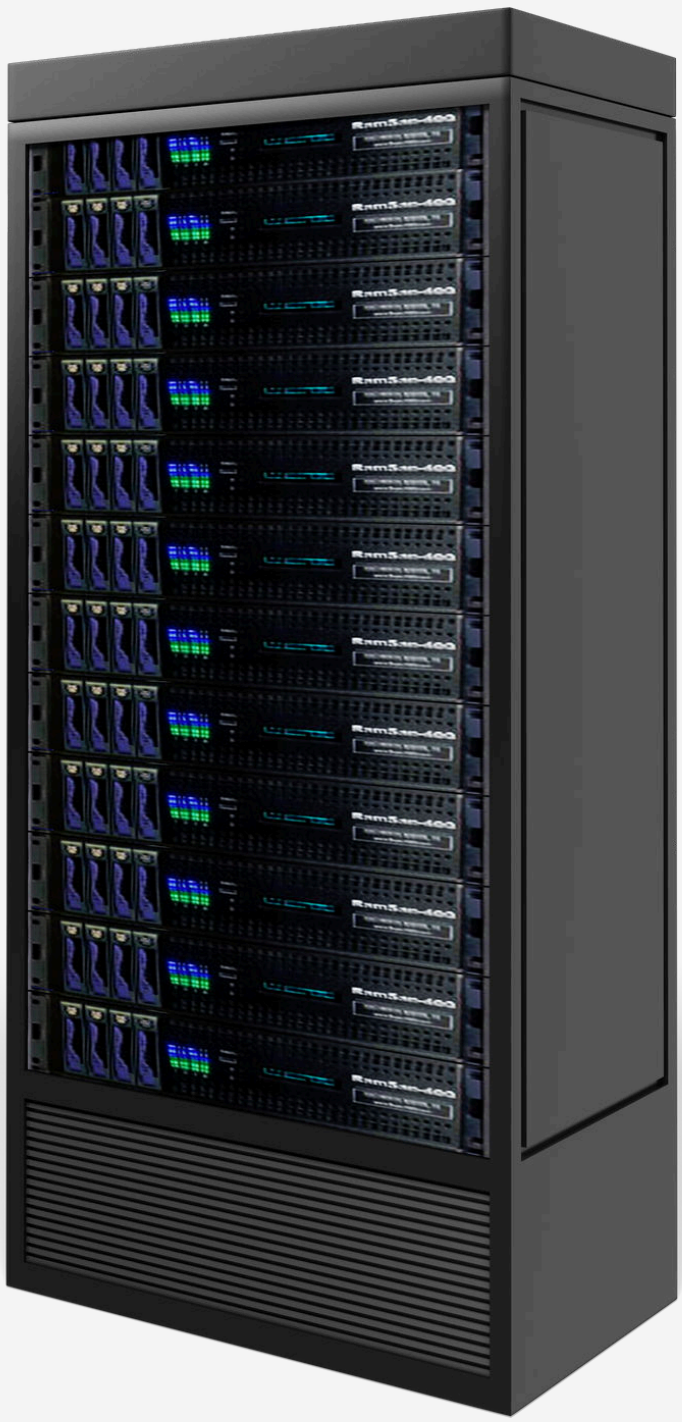
INDEAVOR

7 Strategies for Enhancing Government Cybersecurity

Guide

INDEAVOR

Intro



In 2015, the U.S. Office of Personnel Management (OPM) experienced one of the biggest data breaches in U.S. government history—4.2 million employee personnel files were exfiltrated, alongside the fingerprint data of 5.6 million individuals. Government workforce management systems contain personal data of employees, such as Social Security numbers, home addresses, contact details, and financial information.

Unauthorized access to this data could lead to identity theft or misuse. Schedules and operational details in these systems could reveal the timing and location of employee activities, potentially exposing them to targeted security threats. To protect sensitive information and uphold public trust, maintaining security over internal workforce management and scheduling processes is crucial for government agencies.

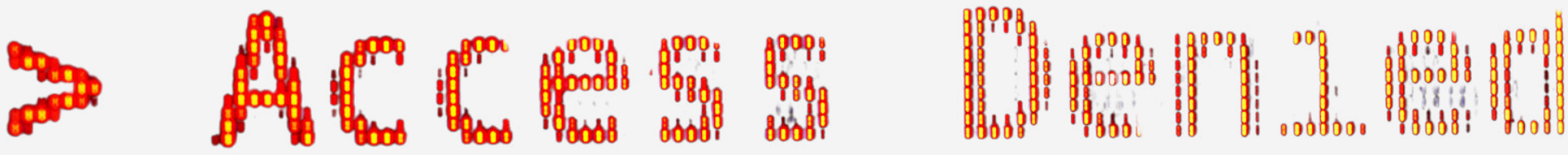
INDEAVOR

#01 ROBUST ACCESS CONTROLS

Establish strict policies that clearly define:

- **Who** can access the system, based on their role within the organization?
- **What** level of access each role is granted, specifying which data sets or system functionalities are available to them?
- **When** access is permitted, potentially include restrictions based on time or location to enhance security further.
- **How** access is granted and monitored, detailing the authentication processes and tracking mechanisms used.

Utilize role-based access controls (RBAC) to ensure that employees only have access to the information necessary for their specific roles. The dynamic nature of government roles—due to promotions, role changes, or personnel turnover—requires ongoing management of access permissions. Be sure to regularly review and adjust access permissions to adapt to changes in roles or responsibilities.



INDEAVOR

ADVANCED USER AUTHENTICATION #02

Advanced user authentication is a critical security layer for protecting sensitive government systems from unauthorized access. It’s important that agencies implement multi-factor authentication (MFA) for accessing sensitive systems and data.

MFA requires users to provide two or more verification factors to gain access to a system, application, or data, enhancing security by adding layers of defense. The factors involved typically include:

- **Something you know:** This could be a password or PIN.
- **Something you have:** This includes devices like a security token, a smartphone app, or an SMS sent to the employee’s phone.
- **Something you are:** This involves biometrics such as fingerprints or facial recognition.

INDEAVOR

#03

SECURE DATA TRANSMISSION AND STORAGE

To protect sensitive information from unauthorized access and leaks, use encryption protocols for data in transit and at rest. Utilize strong encryption protocols such as TLS (Transport Layer Security) for data transmitted across networks.

Every organization is held accountable to different standards of data transmission and storage. Common standards include:

- **Federal Information Processing Standards (FIPS):** Set of standards developed by the U.S. federal government for computer systems used by non-military government agencies and government contractors. They are intended to ensure that systems are secure and interoperable, with specific criteria for encryption algorithms.
- **NIST (National Institute of Standards and Technology):** Comprehensive standards and best practices to help federal agencies manage and protect information systems and data. The guidelines cover a wide range of areas, including cybersecurity, encryption protocols, and risk management processes.
- **General Data Protection Regulation (GDPR):** EU law on data protection and privacy in the European Union and the European Economic Area, addressing the transfer of personal data outside the EU and EEA. GDPR is designed to give individuals control over their personal data.

Implement a robust key management system (KMS) that ensures encryption keys are securely generated, stored, and retired. Automated systems help rotate these encryption keys periodically and revoke them when no longer needed.

INDEAVOR

#04 CONDUCT REGULAR AUDITS

Regularly review and update internal security policies to align with the evolving threat landscape and technological advancements. This includes evaluating procedures for data handling, access control, and incident response.

Schedule routine compliance audits for external regulations (e.g., GDPR for data protection in the EU, HIPAA for healthcare information in the U.S., or other sector-specific standards). Non-compliance can lead to legal consequences, fines, and damage to public trust. You can stay ahead with regular penetration testing and vulnerability assessments.

Penetration testing simulates cyber attacks to identify vulnerabilities in your systems. This proactive approach helps understand the effectiveness of the existing security measures. Vulnerability assessments are systematic reviews of all IT systems, applications, and network infrastructures to identify and categorize risks based on their severity and potential impact.

INDEAVOR

GUIDED SECURITY TRAINING #05

A joint study conducted by Stanford University and Tessian found that a staggering 88% of data breaches are caused by employees. This isn't malicious, just human error. With this in mind, it's important to regularly train all employees on security best practices and the importance of protecting sensitive information.

Develop a training curriculum that covers essential topics such as password management, recognizing phishing attempts, safe internet practices, and secure use of mobile devices. Roles within the agency that require access to highly sensitive information, such as HR, may benefit from specialized training modules tailored to the specific security needs of these roles.

INDEAVOR

#06

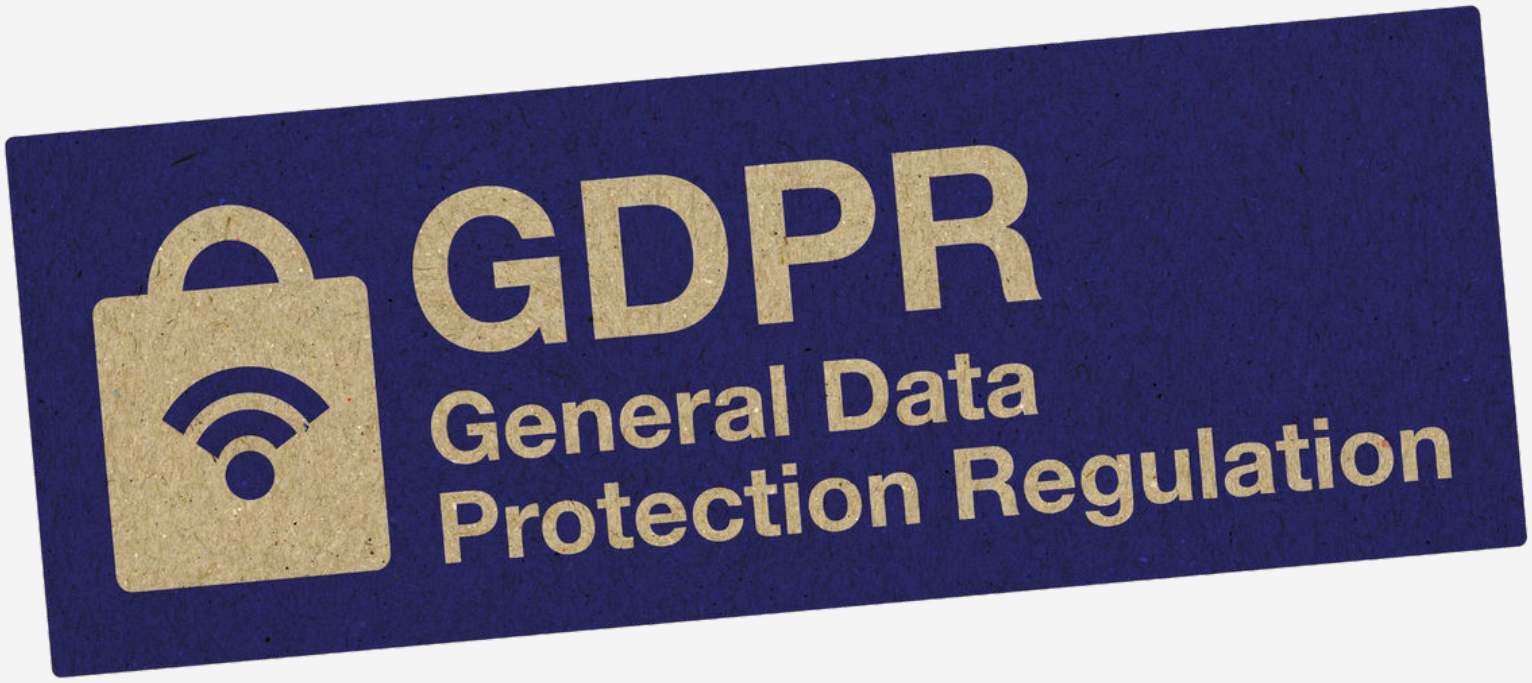
INCIDENT RESPONSE AND RECOVERY PROTOCOLS

Incident response and recovery protocols are crucial components of a comprehensive security strategy, especially in government sectors where the impact of security breaches can be severe. Develop a thorough incident response plan that outlines specific steps to be taken in the event of a security breach. This plan should cover the identification of the incident, containment strategies, eradication of the threat, recovery steps, and a thorough post-incident analysis.

There should be clearly defined roles and responsibilities for all employees involved in incident response. This should include the incident response team, IT staff, legal department, communications team, and executive leadership. Create a response team with members trained in specific aspects of the incident response, such as technical analysis, communication, and legal issues.

INDEAVOR

#07 SOFTWARE WITH BUILT-IN SECURITY



Safeguarding sensitive data and ensuring operational continuity is a must. So the capabilities of whatever workforce management solution you choose (or are already relying on) should be scrutinized. The workforce management and scheduling software should have security measures built-in.

To help enforce strict access policies within the organization, opt for vendors that provide comprehensive security measures like data encryption, secure user authentication, automated activity logging, and role-based access control (RBAC). Assess their compliance with relevant security certifications and standards such as SOC 2 or GDPR.

Finally, the software needs to be able to integrate seamlessly with your existing IT infrastructure without creating new vulnerabilities. Compatibility with other security tools and systems is key.

Indeavor Supports Mission-Critical Agencies

Government agencies can rest assured that their sensitive employee information (e.g., schedules, addresses, etc.) will always remain protected with Indeavor.

- **Certification and Compliance:** Indeavor is compliant with GDPR and SOC 2 Type II. This SOC 2 certification ensures that Indeavor adheres to rigorous standards for security, availability, confidentiality, processing integrity, and privacy, making it reliable for sensitive environments like government operations.
- **Data Protection:** Indeavor's infrastructure is secure. The platform uses advanced encryption to protect data both at rest and in transit, ensuring that all user interactions and stored data are shielded from unauthorized access.
- **Access and Identity Management:** The platform employs strong access controls such as Single Sign-On (SSO) and Multi-Factor Authentication (MFA), which ensure that only authorized users can access sensitive information. They also practice access provisioning according to the least privilege principle and regularly review user access (Indeavor).
- **Regular Security Audits and Vulnerability Management:** Indeavor conducts regular vulnerability management and incident response activities. They also perform penetration testing to identify and mitigate potential security weaknesses.
- **Resilience and Recovery:** Indeavor's infrastructure is designed for high availability and redundancy, with multiple availability zones and disaster recovery protocols in place to minimize downtime and ensure continuous operation.

INDEAVOR

Conclusion

#01 — ***Robust access controls*** *to ensure that only authorized personnel have access to specific information.*

#02 — ***Advanced user authentication*** *to add a second layer of access protection.*

#03 — ***Secure data transmission and storage*** *to protect sensitive information from leaks, whether in transit or at rest.*

#04 — ***Conduct regular audits*** *to identify vulnerabilities within your systems before a real-world attack occurs.*

#05 — ***Guided security audits*** *to avoid accidental data breaches from employees.*

#06 — ***Incident response and recovery protocols*** *to minimize impact, recover swiftly, and maintain public trust.*

#07 — ***Software with built-in security*** *to automate the safeguarding of sensitive data and ensure operational continuity.*

INDEAVOR

Plan. Schedule. Engage. Optimize.

The Modern People Operations Platform for Manufacturing, Consumer Products, Energy and Public Enterprises.

www.indeavor.com