Table of Contents

Employee Responsibilities and Conduct

All employees play a vital role in maintaining Docupal Demo, LLC's cybersecurity posture. Your actions directly impact the security of our data and systems. This section outlines your responsibilities and expected conduct regarding cybersecurity.

Acceptable Use and Expected Behavior

You are responsible for using company resources, including computers, networks, and data, in a secure and responsible manner. This includes:

- Creating strong, unique passwords for all accounts and changing them regularly.
- Protecting your credentials and never sharing them with anyone.
- Being cautious of suspicious emails, links, and attachments, and avoiding clicking on anything that seems untrustworthy.
- Ensuring that you do not disable any security software on company devices.
- Refraining from accessing or attempting to access data that you are not authorized to view.
- Never using company resources for illegal or unethical activities.

Reporting Security Incidents

You are required to immediately report any suspected or confirmed security incidents to the IT Security Department. This includes:

- Phishing attempts
- Malware infections
- Data breaches
- Unauthorized access attempts
- Any other unusual or suspicious activity

Your prompt reporting is crucial for mitigating potential damage and ensuring a swift response.

Access Control and Password Management

Docupal Demo, LLC requires robust access control and password management practices to protect sensitive information. This section outlines the policies and procedures for managing access to company resources and ensuring the security of passwords.

Password Requirements

All employees must adhere to the following password requirements:

- **Complexity:** Passwords must be at least 12 characters long. They need to include a mix of uppercase and lowercase letters, numbers, and symbols.
- **Expiration:** Passwords must be changed every 90 days. Employees will receive reminders before their passwords expire.
- **Uniqueness:** New passwords must not be similar to previous passwords.
- **Storage:** Passwords must never be written down or shared with anyone.
- **Password Managers:** Employees are encouraged to use approved password managers to securely store and manage their passwords.

Access Control

Access to sensitive information is carefully controlled and monitored. Docupal Demo, LLC employs the following measures:

- **Role-Based Access Control (RBAC):** Access to systems and data is granted based on an employee's job role and responsibilities. Employees are only given the access they need to perform their duties.
- **Multi-Factor Authentication (MFA):** MFA is required for accessing critical systems and data. This adds an extra layer of security by requiring users to provide two or more verification factors.
- **Regular Access Reviews:** Access rights are reviewed regularly to ensure they remain appropriate. This helps to identify and remove unnecessary access.
- **Monitoring and Logging:** All access to systems and data is monitored and logged. This allows us to detect and investigate suspicious activity.

Secure Access Tools

Docupal Demo, LLC provides and supports the following tools to facilitate secure access:

- **Virtual Private Networks (VPNs):** VPNs are used to create secure connections when accessing company resources from outside the office network.
- **Multi-Factor Authentication (MFA):** As mentioned above, MFA is a critical tool for enhancing security.
- **Password Managers:** Approved password managers help employees create and store strong, unique passwords.
- **Endpoint Detection and Response (EDR):** EDR solutions are used to monitor and protect endpoints (desktops, laptops, and servers) from cyber threats.

Data Protection and Privacy Guidelines

Docupal Demo, LLC is committed to protecting the privacy and security of all data entrusted to us. These guidelines outline the procedures for handling data in compliance with privacy laws and regulations, including GDPR and CCPA. All employees are responsible for adhering to these guidelines to maintain data confidentiality, integrity, and availability.

Data Handling Procedures

All data must be classified based on its sensitivity:

- **Public:** Freely shareable.
- **Internal:** For internal use only.
- **Confidential:** Requires additional protection.
- **Restricted:** Requires the highest level of security.

Appropriate protection measures, such as encryption and access controls, must be applied based on the data classification. Data minimization and purpose limitation principles must be followed, ensuring that only necessary data is collected and used for specified purposes. Consent must be properly managed, and individuals' rights regarding their personal data must be respected.

Secure Data Disposal

When data is no longer needed, it must be disposed of securely. This includes:

- Physical destruction of storage media.
- Secure wiping of electronic data using approved software.
- Proper shredding of paper documents.

Incident Reporting and Response Procedures

Docupal Demo, LLC requires all employees to promptly report any suspected or confirmed cybersecurity incidents. A cybersecurity incident is any event that jeopardizes the confidentiality, integrity, or availability of our information assets. This includes, but is not limited to, data breaches, malware infections, unauthorized access to systems or data, and denial-of-service attacks.

Employees must report incidents immediately upon discovery. Reports should be made through one of the following channels: contacting the IT help desk, sending an email to security@docupaldemo.com, or calling the IT Security Department directly. When reporting an incident, provide as much detail as possible, including the date and time of the event, a description of what occurred, any systems or data involved, and any potential impact.

The IT Security Department will acknowledge receipt of the incident report within one hour. A preliminary assessment will be conducted to determine the severity and scope of the incident. Critical incidents should be resolved within 24-72 hours, depending on their complexity. The following chart illustrates our incident response times and resolution rates over the past year.

Security Awareness and Training Programs

Docupal Demo, LLC prioritizes a strong security culture. We maintain this through comprehensive security awareness and training programs. These programs ensure all employees understand their roles in protecting company assets and data.

Training Curriculum

Our cybersecurity awareness training covers essential topics. These topics are:

- Phishing awareness
- Password security
- Data classification
- Social engineering
- Malware prevention
- Incident reporting
- Privacy best practices

Training Schedule and Frequency

All employees must complete cybersecurity awareness training annually. We also offer refresher courses quarterly to reinforce key concepts and address emerging threats.

Measuring Training Effectiveness

We measure the effectiveness of our training programs. We use these methods to ensure employees retain and apply the knowledge:

- Post-training quizzes
- Simulated phishing campaigns
- Periodic security audits

Use of Mobile Devices and Remote Work Security

This section outlines the security measures for using mobile devices and remote work setups. All mobile and remote devices must follow the same security standards as company desktop computers.

Securing Devices Outside the Office

When using devices outside the office, employees must use strong passwords and enable auto-lock features. Avoid using public Wi-Fi networks whenever possible. Ensure all software is up to date to protect against vulnerabilities. Using a Virtual Private Network (VPN) is mandatory when accessing company resources remotely. Device encryption and the installation of approved security software are also required.

Bring Your Own Device (BYOD)

For Bring Your Own Device (BYOD) implementations, devices must meet minimum security standards. This includes installing antivirus software, enabling full-disk encryption, and adhering to company password policies. Docupal Demo, LLC reserves the right to remotely wipe any device that does not comply with these standards to protect company data. Regular security audits will be conducted to ensure ongoing compliance.

Acceptable Use and Internet Policy

Docupal Demo, LLC provides IT resources and internet access to support business operations, employee training, and professional development. These resources must be used responsibly and in accordance with this policy.

Permitted and Prohibited Activities

Permitted activities include tasks directly related to your job, approved training programs, and activities that enhance professional skills. Prohibited activities include any illegal actions, using company resources for personal gain, installing unauthorized software, or violating any other company policy.

Monitoring

To ensure compliance, Docupal Demo, LLC monitors employee activity through network traffic analysis, access logs, and Endpoint Detection and Response (EDR) systems. This monitoring helps protect company assets and maintain a secure IT environment.

Consequences of Violations

Violations of this policy may result in disciplinary action, ranging from warnings and mandatory retraining to suspension, termination, and potential legal action. The severity of the consequence will depend on the nature and impact of the violation.

Policy Compliance and Enforcement

Docupal Demo, LLC takes cybersecurity seriously. We ensure ongoing compliance through several methods. These include regular policy updates and annual security audits. We also conduct periodic policy reviews. Vulnerability assessments further strengthen our security. Continuous monitoring of security controls is also in place.

Enforcement Mechanisms

We maintain policy compliance through consistent enforcement. Security audits help us to identify potential issues. We document any breaches that occur. We also take corrective action to address them.

Consequences of Non-Compliance

Failure to comply with this cybersecurity policy can result in disciplinary action. This may include investigation and documentation of the breach. Repeat offenders will face more severe consequences. Employees responsible for significant breaches could face termination.