Security Policy for evdf.org

1. Purpose
The purpose of this policy is to establish security standards to protect the confidentiality, integrity, and availability of information assets on **evdf.org**. This policy applies to all users, systems, and processes that interact with the website.

2. Scope
This policy applies to all employees, contractors, vendors, and third parties who access the systems and data of **evdf.org**. It also includes the use of devices, applications, and network resources connected to **evdf.org**.

3. Data Protection and Privacy

- **Confidentiality**: All sensitive data (e.g., personal, financial) will be encrypted at rest and in transit.
- **User Privacy**: **evdf.org** will comply with global data privacy laws, including GDPR, CCPA, and other applicable regulations, ensuring that personal data is processed lawfully, transparently, and for specific purposes.
- **Data Retention**: User data will only be retained for as long as necessary to fulfill the intended purpose or as required by law.

4. Access Control

- **Authentication**: All users accessing sensitive systems or data will be required to authenticate using secure methods, including multi-factor authentication (MFA).
- **Authorization**: Access to systems and data will be granted based on the principle of least privilege. Only authorized users will have access to specific resources based on their role.
- **Password Management**: Strong password policies will be enforced, requiring a minimum length, complexity, and regular password changes.

5. Security Monitoring

- **Log Management**: All systems will log user activities, security events, and access attempts for review and auditing.
- **Intrusion Detection Systems**: Regular monitoring for potential breaches will be conducted using IDS/IPS systems to detect and respond to threats.
- **Vulnerability Scanning**: Regular vulnerability assessments and penetration testing will be performed to identify and mitigate security risks.

6. Incident Response

- **Incident Reporting**: Any suspected security incident (data breach, malware infection, unauthorized access, etc.) should be reported immediately to the security team.
- **Response Protocol**: A defined incident response plan will be followed to mitigate and recover from security incidents, including communication with affected users, regulatory bodies, and law enforcement when necessary.
- **Post-Incident Review**: After any security incident, a post-mortem review will be conducted to assess the effectiveness of the response and improve future prevention.

7. Network Security

- **Firewall and Network Segmentation**: Firewalls will be used to separate public and internal networks. Sensitive systems and data will be isolated in secure network zones.
- **Secure Communication**: All data exchanges (both internal and external) will be encrypted using strong encryption protocols (e.g., TLS 1.2+).
- **Remote Access**: Secure VPNs or other encrypted channels will be used for remote access to internal systems.

8. Software and Systems Security

- **Patch Management**: All software, operating systems, and applications will be regularly updated with security patches.
- **Application Security**: Secure coding practices will be enforced, and code will be reviewed for vulnerabilities (e.g., OWASP Top Ten).
- **Third-Party Services**: All third-party services and software will be vetted for security compliance before integration with **evdf.org**.

9. Employee Training and Awareness

- **Security Training**: All employees and contractors will undergo regular security training to raise awareness about potential threats (phishing, social engineering, etc.) and how to mitigate them.
- **Policy Acknowledgment**: All personnel must acknowledge and adhere to the security policies and procedures.

10. Physical Security

- **Data Centers**: Physical security measures will be in place to prevent unauthorized access to data centers, servers, or workstations.

- **Device Security**: Laptops, mobile devices, and other portable devices will be secured with encryption, password protection, and remote wiping capabilities.

11. Compliance and Legal Requirements

- **Legal Compliance**: **evdf.org** will comply with relevant data protection and cybersecurity regulations and industry standards, including GDPR, CCPA, PCI-DSS (if applicable), and others.
- **Third-Party Audits**: Periodic third-party audits may be conducted to assess the security posture of the organization.

12. Continuous Improvement

- **Security Assessments**: Regular reviews and updates to the security policy will be conducted to address evolving threats and incorporate best practices.
- **Feedback and Improvement**: Feedback from staff and external security audits will be incorporated into the security policies and practices.