Customer Portal Policy

1. Purpose and Scope

This policy outlines the security measures, roles, and responsibilities related to the use of the Customer Portal at DevEnginner. It applies to all customers accessing the portal to ensure secure interaction and data protection. This policy aims to protect customer data, ensure secure operations, and provide a robust incident response framework.

2. Definitions

- **CSRF (Cross-Site Request Forgery)**: An attack that forces an authenticated user to execute unwanted actions.
- **XSS (Cross-Site Scripting)**: A vulnerability that allows attackers to inject malicious scripts into web pages viewed by users.
- **Zero-Trust Architecture**: A security concept where no one is trusted by default, and strict identity verification is required.
- **MFA (Multi-Factor Authentication)**: A security method that requires more than one method of authentication from independent categories to verify the user’s identity.

3. Roles and Responsibilities

- **Customers**: Must follow portal usage guidelines, report suspicious activities, and maintain strong passwords.
- **IT Team**: Ensures the portal is secure, monitors for incidents, and responds promptly to security events.
- **Support Team**: Assists customers and facilitates incident reporting.

4. Access Control

- Customers are required to use MFA to access the portal.
- Role-Based Access Control (RBAC) ensures users have access only to the necessary resources.
- Passwords must meet security criteria (e.g., length, complexity) and expire periodically.

5. Data Security

- All customer data is encrypted both in transit and at rest using industry-standard protocols.
- Data retention periods are clearly defined, and customer data is securely deleted after the retention period ends.
- Monitoring and logging mechanisms are in place to ensure compliance and detect unauthorized access.

6. Secure Development

- The portal is developed using secure coding practices to mitigate risks like CSRF and XSS.
- Regular vulnerability testing is performed to identify and patch potential security gaps.
- New security features, such as Zero-Trust Architecture, are continuously evaluated for relevance and implementation.

7. Incident Response

- Any security incident affecting the portal will be communicated to customers within 24 hours of detection.
- The incident response plan includes containment, eradication, and recovery steps.
- Customers must report suspicious activity through the portal or by contacting customer support.

8. Monitoring and Logging

- Real-time monitoring and logging of portal activities are conducted to detect and respond to security threats.
- Behavioral analytics are used to identify abnormal behavior that may indicate compromised accounts.

9. Customer Notification

- In the event of a breach, customers will be notified immediately, with details on the nature of the breach, its impact, and steps taken to mitigate it.
- Follow-up notifications will provide further details on corrective actions and any required steps for customers.

10. Third-Party Service Integration

- Third-party integrations are carefully vetted to ensure they meet security standards and do not introduce supply chain risks.
- Continuous monitoring of third-party services is conducted to ensure compliance with this policy.

11. Compliance and Review

- This policy complies with applicable laws and industry standards, including GDPR and other relevant data protection regulations.
- The policy will be reviewed annually or upon any significant changes in the threat landscape or business operations.

12. Enforcement

- Non-compliance with this policy may result in restricted portal access or other actions by the company that are deemed necessary.

Revision History

Date of Change	Responsible	Summary of Change	Next Review
July 2024	Chief Information Officer	Initial creation of policy	January 2025