Title: NovaSoft AWS Usage and Spending Policy

1. Purpose

- This policy defines how NovaSoft teams use AWS accounts and budgets.
- The goal is to control cloud costs while allowing teams to experiment.

2. Account types

- There are three types of AWS accounts at NovaSoft: Development, Staging, and Production.
- Only the Cloud Platform team can create new AWS accounts.
- Each product team is assigned specific accounts for their services.

3. Spending limits

- Development accounts have a spending limit of 500 USD per month.
- Staging accounts have a spending limit of 1,000 USD per month.
- Production accounts are monitored daily; any unexpected spike above 20% of the average monthly bill must be investigated within 24 hours.

4. Who can create resources

- Only engineers with the “DevOps” or “Cloud Admin” role can create or delete AWS resources such as EC2 instances and RDS databases.
- Application developers should use predefined templates and Terraform modules when possible.

5. Tagging requirements

- All resources must include the following tags:
    - Project – project or product name.
    - Environment – Dev, Staging, or Prod.
    - Owner – team or squad name.
- Untagged resources may be shut down after a notification.

6. Cost monitoring

- The Finance team receives a weekly AWS cost report.
- If any account crosses 80% of its monthly budget, a Slack alert is sent to the owning team.
- Teams must review their usage and shut down unused resources.

7. Data security

- Production databases must have automated backups enabled with at least 7 days of retention.
- Access keys should not be hard-coded in source code; use environment variables or secret managers.

8. Environments and data classification

- Development and staging accounts must not contain real customer data.
- Only anonymized or fake test data may be used in non-production environments.
- Production environments are classified as **Highly Sensitive** and follow stricter access rules.

9. Access management

- All AWS access must go through the company's single sign-on system where available.
- Individual IAM users should be avoided; IAM roles and temporary credentials are preferred.
- Access reviews must be conducted at least once every quarter to ensure only required permissions are active.

10. Backup and recovery

- Critical production databases must have automatic daily backups with at least 7 days of retention.
- Backups should be stored in a different availability zone or region where possible.
- Disaster recovery drills should be performed at least once a year to validate restoration procedures.

11. Logging and monitoring

- CloudTrail, CloudWatch, and other logging tools must be enabled for production accounts.
- Logs should be retained for at least 90 days for security investigations.
- Alerts for unusual activities, such as many failed logins or sudden spikes in API calls, should be configured.

12. Use of experimental services

- New or experimental AWS services should first be tried in a sandbox account.
- Before using them in production, the team must review security, cost, and support implications.
- Any service that stores customer data must be reviewed by the security team.

13. Data transfer and egress costs

- Large data transfers out of AWS can generate high egress costs.
- Teams should plan architecture to minimize unnecessary data transfer between regions.
- Bulk downloads of logs or backups should be scheduled during off-peak hours if possible.

14. Third-party tools in AWS

- Any third-party tool that connects to AWS accounts must be reviewed by security and approved by the Cloud Platform team.
- API keys and tokens for such tools must be stored securely and rotated regularly.

15. Violations and corrective actions

- If a team exceeds the defined spending limit repeatedly, a cost review meeting will be scheduled.
- Unsafe configurations, such as publicly exposed databases, must be fixed immediately.
- Serious or repeated violations of this policy may be escalated to senior management.