connectmyapps

IT Security overview

kiwa certified ISO 27001

NORWEGIAN ACCREDITATION MSYS 004

Overview

ConnectMyApps have implemented industry standard security across our business and technology and is GDPR compliant. All data is stored within the EU.

Our platform primarily runs on Amazon Web Services (AWS) in two locations within the EU, with multiple Availability Zones (AZ) to ensure continuous uptime. ConnectMyApps has the second highest support SLA available with AWS and use their advanced tools available to protect against cyberattacks. Our historic uptime is 99.99% excluding scheduled maintenance.

AWS provides CMA with a host of security measures to ensure business continuity and secure storage and transfer of data. Read more on slide 10.

We use AES256 level encryption for data at rest, and only store data for a maximum of 30 days before it is automatically deleted.

ConnectMyApps and Amesto Group (ConnectMyApps' largest shareholder) have dedicated Security Incident Response Teams and documented Disaster Recovery procedures which are tested annually

We prevent unauthorized access to our platform through policies such as “minimum required access” and technical measures such as VPNs, firewalls, access logs, IP address restrictions and two-factor authentication.

All software used is from leading vendors and automatically patched and continuously updated with the latest antivirus and malware software.

ConnectMyApps conduct annual penetration testing for the OWASP Top 10 security threats on our critical infrastructure via an accredited third party. ConnectMyApps is ISO 27001 certified.

This document is divided into the following sections:

ConnectMyApps is part of the Amesto Group and is governed by group IT security policies and procedures. Please see the Amesto Trust Center: https://www.amesto.com/amesto-trust-center/

1000+ staff across Nordics, Europe and USA
1.2 billion NOK revenue in 2024

Responsible for:
Group IT policies and procedures / ISMS
Overall GDPR responsibility
HR policies and procedures
Financial shared services

Responsible for:
Managing IT security on Amesto Group systems

Provide DevOps as a Service to complement ConnectMyApps' internal DevOps team

Responsible for:
IT security on ConnectMyApps specific systems

Standards and Frameworks

- Broadly follow NIST Cybersecurity Framework.
- ISO 27001 certified.
- ISMS in place within Amesto Group including ConnectMyApps.
- System Owners are required to review access every quarter and documentation review is performed annually.
- ConnectMyApps is compliant with GDPR rules and regulations
- DPAs with all software vendors used by ConnectMyApps that are ultimately owned by US companies include Standard Contractual Clauses, and in most cases have Binding Corporate Rules in place.
- Follow Privacy by Design principles when developing integrations e.g. minimize the fields and data transferred to only those absolutely required; only store data absolutely required for technical support purposes; automatically delete all records after 30 days; meta data used for platform maintenance is anonymized etc.

System hardening

- ConnectMyApps enforces a user minimum password policy of 8 characters, with mandatory numbers, special characters and capital letters.
- All staff required to use secure password generator applications
- Maximum 3 attempts allowed to login after which account is locked.
- Access to internal systems via internal VPN only, with enforced two-factor authentication.
- Access is logged and monitored.
- Minimum requirements on password enforced. Internal logins stored and managed in AWS secrets manager
- AWS access managed via IAM with auto-rotation of keys. Policy for deletion of inactive users.
- Employee hardware such as laptops and smart phones enrolled in Amesto security policy (Microsoft Intune) and can be wiped remotely by Amesto Group IT Operations.
- Malware and antivirus protection from industry leading vendor installed on all laptops.

Platform security

- Security audit and penetration testing for OWASP Top 10 security threats is performed by an accredited external third party (Digital X Raid) annually.
- The ConnectMyApps platform is hosted in Amazon Web Services (AWS) with multiple AZ's (Availability Zones) located in Frankfurt with backup in Dublin. ConnectMyApps has second highest AWS support SLA available.
- Access to administration of the AWS platform is controlled by multi-factor authentication and IP restriction.
- Database backups are performed once per day as "hot snapshots".
- Communication to server instances is conducted via an elastic load balancer (ELB), reducing the risk of "single point of failure."
- Automatic health checks performed on the servers every minute. Faulted server instances are removed, and new servers are automatically provisioned if required.
- Inter-process communication within the platform is conducted via durable message queues.
- AWS WAF (Web Application Firewall) used as an external firewall on key public facing APIs and application endpoints.
- AWS Shield used to mitigate and prevent DDoS attacks.
- Servers within the platform are updated automatically via Microsoft security updates. Databases in AWS are auto-patched and updated and part of AWS RDS service.
- SSL certificates used by ConnectMyApps are managed in AWS Certificate Manager and renewed automatically.
- ConnectMyApps uses the latest development software, such as Microsoft Visual Studio 2022, and latest Windows operating systems. We closely monitor the technology landscape for changes and updates, including new security updates. ConnectMyApps has a Change Management Team that has a formal procedure for emergency changes.
- Malware and antivirus software provided by industry leading vendor.
- Amesto services run in Azure and AWS have IDS and IPS systems such as Azure Firewall and Security Center.
- We work with Procano, who provide DevOps as a Service to complement our internal DevOps team.

Data storage and encryption

- All HTTP traffic between the ConnectMyApps platform and the public internet is encrypted with SSL certificates. Certificates are managed via AWS Certificate Manager with automatic renewal and rotation.
- The ConnectMyApps platform uses TLS 1.3 for incoming connections.
- Access to the AWS platform is managed by AWS IAM (Identity and Access Management). User access is provisioned by the Dev Ops manager. Access keys are rotated every 90 days.
- Static data within the ConnectMyApps platform is automatically encrypted at rest using AES256 encryption.
- Data transferred via the ConnectMyApps platform is either transited without being stored or is stored for a maximum of 30 days before automatic deletion, depending on the requirement of the integration.
- Customers can elect to not have data stored at all, though this limits the possibility to provide certain levels of technical support.
- User passwords are “salted” and encrypted via one-way hash encryption algorithm prior to storage. User accounts lock after three unsuccessful login attempts and may only be opened by ConnectMyApps support team.
- ConnectMyApps is a multi-tenant platform. Users are separated by a globally unique ID. Platform API access is IP restricted by default.
- Files shared between customers and ConnectMyApps support team are transferred via a secure file sharing application, not email.

Access Right restrictions

- Access rights to applications and systems is granted and controlled by the CTO with a policy of “minimum required access rights”.
- Critical production systems have two-factor authentication enabled, meaning those with access need a login and one-time time code generated by authenticator app. Access is restricted to the IP address of the VPN, so it is not possible to connect unless on VPN.
- Internal production logins are stored encrypted in AWS Secrets Manager.
- VPN access is controlled by ConnectMyApps DevOps Manager and CTO. ConnectMyApps logs all access to the VPN.
- Credential usage is logged and can be disabled if compromised. Rotate keys on schedule, check for IP address ranges and block if needed. Amazon Key Management Service used to manage and rotate cryptographic keys.
- AWS Cloudwatch used for event and access logging across the entire ConnectMyApps platform, as well as for automatic alerting in the event of resource usage spikes, access attempts and as a platform-wide audit log.
- AWS SNS (Simple Notification Service) employed for alerting of incidents. Major incidents automatically routed to appropriate personnel.
- Access to customer information is limited for the individual customer i.e. they can only see their own data. Authentication is confirmed via username / password, two-factor authentication, or a unique API key set for programmatic access.
- Customer API access is controlled by default with IP address whitelisting.
- Customer user passwords are “salted” and encrypted via one-way hash algorithm.
- Customer application passwords are encrypted using unique “per customer” encryption key.
- Employee devices are protected by multi-factor authentication.
- Proactive vulnerability checks, and reactive machine learning based Endpoint Detection and Response measures for end user devices.

Staff training

- ConnectMyApps conducts annual GDPR and Privacy training and refresher courses to all employees.
- All employees have confidentiality clauses in their employment contracts.
- New employees are given GDPR training as part of their onboarding procedures.
- All employees have access to and are required to read the Data Privacy handbook accessible in our shared Data Privacy folder.
- Amesto Group conduct regular, compulsory Data Privacy training for staff.
- Internal hotline for Amesto Group personnel to report security incidents.

Physical access

- Access to premises is restricted by key card access with photo ID. All visitors must be registered and accompanied by staff at all times.

Disaster recovery

ConnectMyApps takes the following broad disaster recovery measures:

- Managed by defined Incident Response team in ConnectMyApps
- Escalation procedures to Amesto Group IT Ops for security incidents in place.
- Regular daily automated snapshots of production databases. Backups stored 30 days back in time.
- Application server volumes backed up automatically using AWS DLM (Data Lifecycle Manager).
- Application servers and backend servers separated into public and private VPC subnets. Application servers fronted by Elastic Load Balance.
- Disaster recovery plan in place to replace compromised or failing servers.
- Disaster recovery training is performed annually.

AWS Resources

Amazon Web Services (AWS) provides CMA with the infrastructure on which our Canvas service operate.

AWS guarantees all data entrusted to CMA by its customers is exclusively stored in the EU and provides us with integral components of the information security CMA guarantees for its customers.

AWS supports 143 security standards and compliance certifications, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-3, and NIST 800-171.

For more details, please visit AWS Security and Compliance Center:

- AWS Data-center Controls https://aws.amazon.com/compliance/data-center/controls/
- AWS Compliance: https://aws.amazon.com/compliance/
- AWS Artifact: https://aws.amazon.com/artifact/getting-started/
- AWS Shared Responsibility Model: https://aws.amazon.com/compliance/shared-responsibility-model/