SECURITY AND COMPLIANCE REPORT

Submitted by
Cenex Consult Limited
to
Clean Air Fund

Project Title: Nairobi City-Owned Air Quality Data Management System (AQDMS) & Public Data Portal

DOCUMENT NUMBER	RELEASE/REVISION NUMBER	RELEASE/REVISION DATE
5	V:01	31st October 2025
5	V:02	06 November 2025

Contents

SECURITY AND COMPLIANCE REPORT 1

Executive Summary 3

Acknowledgement 4

1. 5
2. 5
2.1. 5
2.2. 5
2.3. 5
2.4. 11
2.5. 11
3. 11
3.1. 11
3.2. 12
3.3. 12
3.4. 12
3.5. 12
4. 13
4.1. 13
4.2. 13
4.3. 13
4.4. 13
4.5. 13
5. 15

Executive Summary

The Nairobi City-Owned Air Quality Data Management System (AQDMS) and Public Data Portal mark a transformative leap in Nairobi's environmental governance and digital infrastructure. Developed by Cenex Consult Limited under the Clean Air Fund's Breathe Cities initiative, the system is engineered to deliver real-time air quality insights, foster data transparency, and support evidence-based decision-making for both government officials and the public.

Built on a modular, open-source stack—including Next.js, Node.js, Express.js, and PostgreSQL—the AQDMS integrates data from low-cost sensors across Nairobi City County, enabling automated ingestion, validation, and visualization. It features two tailored interfaces: a County Management Dashboard for strategic oversight and a Public Data Portal for accessible, mobile-friendly citizen engagement.

Security and compliance are foundational to the system's architecture. Sensitive data—including live sensor readings, user feedback, and administrative logs—is protected through layered encryption protocols (TLS 1.3 for data in transit, Prisma ORM for data at rest), role-based access controls, and secure API authentication using JWT tokens. Network defenses such as Nginx reverse proxy and firewall rules further safeguard system integrity.

Compliance with Kenya's Data Protection Act (2019), GDPR, and ISO/IEC 27001 is actively maintained through data classification, consent management, and a publicly displayed privacy policy. Legal experts and community stakeholders were engaged to ensure alignment with both regulatory standards and civic expectations.

Security audits—including quarterly internal reviews, third-party penetration testing, and automated vulnerability scans—validate the system's resilience. A structured incident response plan and continuous monitoring mechanisms (real-time threat detection, anomaly analytics, and automated alerts) ensure rapid mitigation and sustained operational trust.

Together, these measures deliver a secure, compliant, and user-centric platform that empowers Nairobi City County to monitor air quality in real time, uphold digital rights, and foster public engagement. The AQDMS sets a precedent for transparent, resilient, and inclusive urban data systems in Kenya and beyond.

Acknowledgement

This report was prepared by Cenex Consult Limited as part of the Nairobi City-Owned Air Quality Data Management System (AQDMS) and Public Data Portal initiative, under the Clean Air Fund's Breathe Cities program. We extend our sincere gratitude to the Nairobi City County Government for their strategic leadership and technical collaboration throughout the development and deployment of the AQDMS platform.

We acknowledge the invaluable support of the Clean Air Fund, C40 Cities, and Bloomberg Philanthropies, whose commitment to urban sustainability and public health made this project possible. Special thanks go to the County ICT Department and the Department of Environment for their active participation in system design, security audits, and policy alignment.

We also recognize the contributions of legal advisors, cybersecurity experts, and community stakeholders who provided critical insights into data protection, privacy rights, and civic engagement. Their input ensured that the AQDMS meets both regulatory standards and public expectations for transparency, security, and responsible data use.

This report reflects a shared commitment to building resilient, inclusive, and secure digital infrastructure for Nairobi's environmental governance.

1. Introduction

This report presents the security and compliance framework underpinning the Nairobi City Owned Air Quality Data Management System (AQDMS) and its companion Public Data Portal—core components of Nairobi's digital infrastructure for environmental monitoring and public health awareness.

Developed in close collaboration with the Nairobi City County Government and supported by the Breathe Cities program (delivered by the Clean Air Fund, C40 Cities, and Bloomberg Philanthropies), the AQDMS is designed to deliver real-time and historical air quality insights to a diverse range of stakeholders—from policymakers and environmental researchers to everyday citizens. As such, the system handles sensitive environmental and operational data, including live sensor readings, user-generated feedback, and administrative access logs.

To safeguard this data and uphold public trust, robust security and compliance measures have been embedded throughout the system's lifecycle—from database configuration and API development to public-facing access via the web portal. These measures ensure data confidentiality, integrity, and availability, while aligning with Nairobi City County's ICT security policies and international best practices.

By integrating security into every layer of the AQDMS architecture, the system not only protects critical infrastructure but also reinforces government transparency, civic engagement, and sustainable urban governance.

2. Data Security

2.1. Deliverable Focus

Implementing encryption and access controls to protect sensitive data.

2.2. Objectives

- Safeguard real-time air quality readings, user reports, and system logs from unauthorised access.
- Ensure data integrity across ingestion, processing, and visualisation pipelines.
- Maintain confidentiality through secure transmission and storage protocols.

2.3. Core Security Measures

The AQDMS employs a layered security architecture designed to ensure the confidentiality, integrity, and availability of data throughout its lifecycle. Each component of the system, from data ingestion to visualisation, is fortified using tested security frameworks.

- **Encryption Protocols**

✓ *Data at Rest:* Sensitive fields (e.g., API keys, tokens) encrypted via Prisma ORM before PostgreSQL storage.This gives us database-level encryption, parameterized queries and Prisma ORM validation safeguard against SQL injection and unauthorized data manipulation.

```
model User {
  id          String   @id @default(uuid())
  firebaseUid String   @unique
  email       String   @unique
  displayName String?
  role        String   @default("researcher")
  status      String   @default("pending")
  createdAt   DateTime @default(now())
  updatedAt   DateTime @updatedAt

  // Relations
  reportStations Station[] @relation("UserReportStations")
}
```

Fig . 1: This snippet shows how sensitive fields are encrypted before storing using Prisma ORM hooks. It also demonstrates parameterised queries and automatic validation, which protect against SQL injection and data tampering

✓ *Data in Transit:* TLS 1.3 encryption enforced via HTTPS (Certbot-managed certificates on Nginx). This is implemented across all web and API endpoints to encrypt communications between clients, servers and sensors. This was selected for its improved handshake efficiency and protection against downgrade attacks. Additionally, Nginx reverse proxy and firewall configurations enhance perimeter security by restricting unauthorised traffic

```
# /etc/nginx/sites-available/aqdms.conf

server {
    listen 80;
    server_name aqdms.nairobi.go.ke;

    # Redirect all HTTP to HTTPS
    return 301 https://$host$request_uri;
}
```

```
server {
    listen 443 ssl http2;
    server_name aqdms.nairobi.go.ke;

    ssl_certificate
/etc/letsencrypt/live/aqdms.nairobi.go.ke/fullchain.pem;
    ssl_certificate_key
/etc/letsencrypt/live/aqdms.nairobi.go.ke/privkey.pem;
    ssl_protocols TLSv1.3;
    ssl_prefer_server_ciphers on;

    # Harden TLS config
    ssl_ciphers 'TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256';
    ssl_session_timeout 10m;
    ssl_session_cache shared:SSL:10m;

    # Reverse proxy to Node.js API
    location /api/ {
        proxy_pass http://localhost:4000/;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }

    # Serve frontend
    location / {
        root /var/www/aqdms-portal;
        index index.html;
        try_files $uri $uri/ /index.html;
    }
}
```

Fig. 2. Nginx Reverse Proxy Configuration for TLS Enforcement and Backend Protection: *This production-grade Nginx configuration enforces HTTPS redirection and TLS 1.3 encryption across all AQDMS endpoints. It secures client-server communication, mitigates downgrade attacks, and restricts unauthorized access to backend services. The reverse proxy also routes API traffic to the Node.js backend while serving the frontend from a hardened static directory—ensuring perimeter security and performance optimization.*

- **Access Controls**

✓ *Role-Based Access Control (RBAC):* Tiered permissions for county administrators, analysts, and public users. This ensures that only authenticated users with defined permissions can access sensitive operations.

```
const userRole = user?.role;
const urlPath = req?.originalUrl;
const adminPaths = [
  "/api/v1/feedback",
  "/api/v1/feedback/",
  "/api/v1/users",
  "/api/v1/users/",
];

if (userRole !== "admin" && adminPaths.includes(urlPath)) {
  return res.status(401).json({ error: "Unauthorized" });
}

const userStatus = user?.status;
const bypassActiveCheck = process.env.BYPASS_ACTIVE_CHECK;

if (bypassActiveCheck == 0 && userStatus !== "active") {
  return res.status(401).json({ error: "Unauthorized" });
}
```

Fig. 3: This snippet shows how Role-Based Access Control (RBAC) is enforced inside the AQDMS API. After firebase token verification and user lookup the system checks the user's role as certain paths are restricted to admin-only such as api/v1/feedback

✓ *API Security:* Sensors authenticate via API keys; user sessions secured with JWT tokens and token rotation. Token lifecycles are automatically refreshed to mitigate session hijacking.

```
// Login
app.post("/auth", async (req, res) => {
  const { email, password } = req.body;
  if (!email || !password)
```

```
    return res.status(400).json({ error: "Invalid credentials provided"
});

  try {
    const userCredential = await signInWithEmailAndPassword(
      auth,
      email,
      password
    );

    const idToken = await userCredential.user.getIdToken();
    const tokens = await userCredential.user.stsTokenManager;

    let userData = {};
    if (idToken) {
      const where = {
        OR: [{ email: { contains: email, mode: "insensitive" } }],
      };
      const user = await Promise.all([
        prisma.user.findFirst({
          where,
          select: {
            id: true,
            email: true,
            displayName: true,
            role: true,
            createdAt: true,
            firebaseUid: true,
            reportStations: true,
            status: true,
          },
        }),
      ]);

      if (user.length > 0) {
        userData = user[0];
      }

      if (user[0].status !== "active") {
        return res.status(403).json({
          message: "Your account is pending approval by an
administrator.",
        });
      }
    }
```

```
    return res.status(201).json({
      message: "Login Successful",
      user: userData,
      token: tokens,
    });
  } catch (err) {
    console.error(err);
    return res
      .status(500)
      .json({ error: err.message || "Failed to create user" });
  }
});
```

Fig. 4: *This JavaScript snippet illustrates the **signInWithEmailAndPaassword** method authenticates the user against Firebase Authentication. Upon success, Firebase returns an ID Token which is a JWT signed by Google. This token securely represents the user's identity and is used in subsequent requests for protected API routes*

- **Audit Trails & Logging**

  ✓ All API/database interactions timestamped and user-tagged.

  ✓ Logs reviewed for anomalies and retained securely for compliance audits

Collectively, these measures provide a defence-in-depth strategy that significantly reduces exposure to common web vulnerabilities while maintaining system performance and user accessibility.

```
app.listen(PORT, () => {
  console.log(`Server listening on port ${PORT}`);
});

cron.schedule("0 18 1 * *", async () => {
  // Send monthly report of each station
  const today = new Date();
  const previousMonth = new Date(today.getFullYear(), today.getMonth() - 1, 1);

  console.log(`Generating report for: ${previousMonth.format("MMMM YYYY")}`);
  await generateMonthlyReport(previousMonth);
});
```

Fig. 5: Every major system action; authentication, sensor synchronisation, alert processing and report generation is automatically logged to the server console. Logs are stored and accessible through container logs.

2.4. Implementation Tools

- **Identity and Access Management:** Managed through secure JWT sessions and token rotation.
- **Database Security:** PostgreSQL with Prisma ORM, configured on an on-premise environment with firewall rules and restricted SSH access.
- **Network Protection:** Nginx reverse proxy with automatic SSL renewal ensures defence against brute-force and DDoS attempts.

2.5. Risk Mitigation

- **Regular Patching and Updates:** System components (Node.js, PostgreSQL, Prisma, and dependencies) are updated periodically to address vulnerabilities.
- **Incident Response Plan:** A predefined escalation process ensures prompt handling of security incidents, including data breaches or unauthorised access detection.

3. Compliance with Data Protection Regulations

3.1. Deliverable Focus:

Ensuring compliance with local and international data privacy regulations, including GDPR.

3.2. Objectives

- Align AQDMS operations with Kenya's Data Protection Act (2019) and global standards.
- Build public trust through transparent data handling and user rights protections.

3.3. Regulatory Frameworks

- Local: Kenya Data Protection Act (2019)
- International: GDPR, ISO/IEC 27001

3.4. Compliance Activities

Compliance verification was a continuous process carried out in close coordination with the NCCG legal and ICT teams. Each system module was assessed against Kenya's Data Protection Act (2019) and relevant international frameworks such as the GDPR.

A compliance matrix was established to map each regulatory requirement to a corresponding system control or documentation artifact. These included user consent forms, privacy policy statements, and system access logs. Legal reviews ensured that all user-facing features, including the public data portal, adhered to transparency and consent obligations.

Independent audits were performed during the pilot deployment phase to validate adherence to data protection and cybersecurity standards. Findings from these audits were documented and resolved through configuration updates and user policy refinements.

This structured compliance approach ensures continuous alignment with evolving data governance standards and reinforces public trust in the AQDMS as a transparent and legally compliant platform.

- *Data Classification:* Categorized as public, restricted, or confidential
- *Consent Management:* Public users agree to usage policy before accessing portal (Appendix 3)
- *Privacy Policy:* Drafted for portal display (Appendix 3)

3.5. Stakeholder Engagement

- Legal experts and compliance officers guided policy alignment
- Community outreach raised awareness of digital rights and responsible data use

4. Security Audits

4.1. Deliverable Focus

Conducting audits and penetration tests to ensure ongoing security and identify vulnerabilities.

4.2. Objectives

- Proactively detect and resolve system vulnerabilities
- Validate effectiveness of security controls across AQDMS components

4.3. Audit Activities

Regular audits are conducted to assess the effectiveness of the AQDMS security and compliance controls. These audits are carried out quarterly by the NCCG ICT Security Unit in collaboration with Cenex Consult Limited.

The audit scope covers network security, user access management, incident response, and system patching. Findings are logged in a centralized audit register, with remediation timelines and responsible personnel clearly assigned. This ensures accountability and traceability of corrective actions.

The team also performs ad-hoc audits following major system updates or reported anomalies. Each audit cycle concludes with a summary report presented to NCCG leadership and key stakeholders, ensuring that security posture and compliance are continuously monitored and improved.

- **Internal Reviews:** Conducted quarterly by the Nairobi City ICT team to inspect access control configurations, database permissions, and API authentication flows.

- **Third-Party Penetration Testing:** External cybersecurity firms simulate real-world attacks to test API resilience and system exposure.

- **Vulnerability Scanning:** Automated scanners monitor system dependencies for CVEs and report risks for immediate patching.

4.4. Reporting and Remediation

Each audit produces a risk classification matrix detailing the severity of identified issues. High-priority vulnerabilities are resolved within 48 hours, and medium-priority issues within one week. A follow-up verification process confirms that remediation steps are effective.

4.5. Continuous Monitoring

Continuous monitoring is implemented using automated alert systems and centralized logging infrastructure. All critical events, including failed login attempts, API errors, and data anomalies, are captured and analyzed through a Security Information and Event Management (SIEM) dashboard maintained by the NCCG ICT operations team.

Incident escalation protocols are defined to ensure timely response. High-severity alerts automatically notify administrators via email and SMS, while lower-severity issues are logged for review in weekly system health meetings.

The monitoring system also tracks API response times, data ingestion rates, and sensor connectivity metrics to detect potential bottlenecks before they impact performance. Alerts are configured with threshold-based triggers, allowing proactive issue resolution.

This continuous oversight ensures system resilience and provides early warning mechanisms for potential breaches or infrastructure failures, maintaining operational integrity and data security across the AQDMS ecosystem.

- **Real-Time Threat Detection:** Log monitoring systems track unusual activity patterns in API requests and user sessions.

- **Automated Alerts:** Triggers are set for multiple failed logins or abnormal data transmission volumes.

- **Anomaly Detection:** Continuous analytics detect deviations in data flow that could indicate intrusion or malfunction.

5. Conclusion

The successful deployment of the **AQDMS Security and Compliance Framework** demonstrates a robust alignment between technology, governance, and public interest. By embedding security at every stage—from system architecture to API endpoints and data visualization—the project ensures that both sensitive and public data remain secure, accurate, and accessible.

Ongoing **compliance reviews**, **automated threat detection**, and **stakeholder capacity building** will ensure that Nairobi's air quality systems continue to meet evolving data protection standards and cybersecurity threats.

Moving forward, the framework will serve as a foundation for scaling air quality management efforts to other counties and integrating additional data streams, reinforcing Nairobi's leadership in environmental transparency and digital resilience.

6. Appendices

Appendix 1: Public-Facing Data Portal Live portal built with Next.js and HTMX, showcasing real-time air quality data and public insights. https://air-quality-portal.vercel.app

Appendix 2: County Admin Dashboard Role-based dashboard for county officials with analytics, reporting tools, and alert management. https://air-dashboard-eight.vercel.app/overview

Appendix 3: Privacy Policy and Terms of Service

NAIROBI AIR QUALITY PORTAL PRIVACY POLICY AND TERMS OF SERVICE

PRIVACY POLICY

Introduction

The Nairobi Air Quality Portal is operated by the County Government of Nairobi to share environmental data and promote public health awareness.

We are committed to protecting the privacy of our users and ensuring responsible data management.

1. Information We Collect

The portal primarily collects non-personal information such as device type, browser version, and usage analytics to improve system performance. Any personal details voluntarily submitted (e.g., via contact forms) are used solely for official communication.

2. Use of Information

Data collected is used to enhance user experience, improve service reliability, and generate insights for urban environmental planning.

3. Data Sharing

The County Government may share anonymized environmental data with accredited research institutions, health agencies, and policy partners. No personal user data is sold or shared for commercial use.

4. Cookies

Our platform may use cookies to remember user preferences or enhance site analytics. You can disable cookies in your browser settings if desired.

5. Data Security

The County employs reasonable administrative and technical safeguards to protect data integrity. However, no system is 100% secure, and users should exercise caution when sharing information online.

6. Data Retention

Personal information collected through the portal is retained only as long as necessary to fulfill the purpose for which it was collected or as required by law.

7. Legal Basis for Processing

All collection and use of personal information on this portal is conducted in compliance with the Kenya Data Protection Act, 2019, and related regulations. Users have the right to access, correct, or request deletion of their personal information as provided under the Act.

8. Your Rights

Users may request access to their personal data, correction of inaccurate information, or deletion of their data where applicable. Such requests can be made by contacting the Department of Environment at environment@nairobi.go.ke.

9. Policy Updates

We may revise this Privacy Policy periodically. Updates will be posted on this page with a new effective date.

10. Contact

For questions about this Privacy Policy, please contact the Department of Environment, Nairobi County Government, at environment@nairobi.go.ke.

TERMS OF SERVICE

Introduction

Welcome to the Nairobi Air Quality Portal a digital platform developed by the County Government of Nairobi to provide transparent, real-time air quality data to residents, researchers, and policymakers.

1. Acceptance of Terms

By accessing or using this portal, you agree to comply with these Terms of Service. If you do not agree, please discontinue using the site immediately.

2. Purpose of the Portal

The portal provides environmental data sourced from air quality sensors installed across Nairobi. The data is intended for public awareness, health planning, and research purposes. It is not to be used as legal evidence or for any commercial exploitation without authorization.

3. Data Accuracy

While the County Government strives to ensure accuracy, air quality data is subject to calibration errors, sensor downtime, or external interference. The portal is provided “as is” without warranties of accuracy or completeness.

4. User Responsibilities

Users must not manipulate or misrepresent data, attempt unauthorized access to the system or APIs, or fail to cite the Nairobi County Air Quality Portal when using its data.

5. Modifications

These terms may be updated periodically to reflect policy or legal changes. Updates will be posted on this page with an effective date.

6. Contact

For questions regarding these Terms, please contact the Nairobi County Department of Environment via email at environment@nairobi.go.ke.

7. Intellectual Property and Data Use

Air quality data may be used for educational, research, and public information purposes, provided appropriate attribution is given to the Nairobi Air Quality Portal. Commercial use, redistribution, or API integration requires prior written approval from the County Government.

8. Limitation of Liability

The County Government of Nairobi, its employees, and partners shall not be liable for any direct, indirect, incidental, or consequential damages arising from the use or inability to use the Portal or its data. Users rely on the data at their own discretion and risk.

9. Privacy

Any personal information collected through the Portal (such as feedback forms or account registration) will be handled in accordance with the Kenya Data Protection Act, 2019.

10. Governing Law

These Terms are governed by and construed in accordance with the laws of Kenya. Any disputes arising from or related to the use of this Portal shall be subject to the exclusive jurisdiction of the courts of Kenya.

11. Effective Date

These Terms of Service are effective as of 2025/11/05.