

# Global Good Practices in IoT

(May 2025)

Since the IGF in Hyderabad in 2008, the Dynamic Coalition on the Internet of Things (DC-IoT) has engaged in debate at (and in between) IGFs on the usefulness of Internet of Things, its applicability to help address global and local societal challenges, and the steps that must be taken if the Internet of Things is to develop in a way that serves the global public interest. These debates culminated in draft Global Good Practice Guidelines in 2018. During IGF 2024 in Riyadh the DC IoT reflected on the GPP and suggested (1) to be more concise; and (2) include a reflection on emerging technologies. This resulted in the guidelines reflected below.

## 1. Data Governance

**Data Privacy and Compliance:** Organizations must comply with regulations that may have global impact, such as GDPR, CCPA, and ISO/IEC 27701 to ensure responsible data handling. Best practices include data minimization, clear user consent and robust encryption. Additionally, ethical guidelines should be embraced to ensure a sustainable and equitable digital future.

**Data Ownership and Access Control:** Clear ownership policies for data collected by IoT devices are crucial. Role-based access control (RBAC) and Least-privilege access ensures that only authorized individuals have access to sensitive data. Users must also control personally identifiable data, including sharing and encryption.

**Data Integrity and Transparency:** Ensuring the verifiability and integrity of data collected by IoT devices is essential. Blockchains and immutable ledgers can enhance transparency and trust. Meaningful transparency should give users clear and accessible terms for data usage, tracking, and sharing.

**Impact of AI and Quantum Computing:** Currently, AI can provide automated data classification, anomaly and breach detection and compliance monitoring, including compliance with privacy standards. Quantum computing can threaten this by potentially defeating current encryption methods, necessitating quantum-resistant cryptographic techniques to maintain data security.

## 2. Cybersecurity

**Device Authentication and Encryption:** All IoT devices should use strong authentication protocols, including mutual Transport Layer Security (mTLS) and public key infrastructure (PKI). Data transmission should be encrypted using AES-256 and TLS 1.3. Security must be built into IoT systems from the design phase onward.

**Secure Software Development Lifecycle (SDLC):** Security must be embedded from design to deployment, through regular threat modeling, vulnerability testing and patching. Adopting a "secure by design" approach reduces attack surfaces. Secure update mechanisms should be in place to protect legacy systems.

**Network Security and Monitoring:** Implementing network segmentation, firewalls, and intrusion detection systems (IDS) can help to mitigate many risks. Continuous monitoring using AI-driven security analytics can enhance threat detection – yet may also be used by attackers so continuous attention will be needed. Additionally, proactive risk assessments and cybersecurity frameworks must be implemented to maintain trust – based on a risk management approach.

**Zero Trust Architecture (ZTA):** IoT networks should follow a zero-trust approach, requiring constant verification of device and user identities before granting access.

**Modern Internet Security Standards:** Utilizing state-of-the-art internet security protocols enhances IoT security:

- **DNSSEC (Domain Name System Security Extensions):** Protects IoT devices from DNS spoofing and cache poisoning attacks, ensuring integrity and authenticity of domain name resolutions.
- **DANE (DNS-Based Authentication of Named Entities):** Strengthens IoT device authentication by leveraging DNSSEC to validate TLS certificates, reducing reliance on potentially compromised Certificate Authorities.
- **TLS (Transport Layer Security):** Enforces encrypted communications between IoT devices, ensuring data confidentiality and preventing man-in-the-middle attacks.
- **RPKI (Resource Public Key Infrastructure):** Secures IoT networks against BGP hijacking by verifying the authenticity of IP address announcements, ensuring stable and trusted device communications.
- **ROA (Route Origin Authorization):** Enhances IoT traffic security by preventing unauthorized route announcements, securing network infrastructure from traffic interception or redirection.

**Impact of AI and Quantum Computing:** AI can enhance cybersecurity by enabling predictive threat detection and automated response mechanisms. However, quantum computing poses a serious risk to traditional encryption methods, requiring the urgent development of post-quantum cryptographic solutions to maintain secure communications in IoT networks. Threats and promises go beyond encryption (e.g. quantum machine learning). There will need to be a balance between security by design and learning by doing.

### 3. Resilience and Availability

**Failover and Redundancy:** IoT systems should be designed with redundancy to ensure business continuity. Edge computing can help maintain operations during cloud disruptions. Disaster warning systems and dynamic traffic management should be integrated into IoT deployments to enhance resilience. While resilience needs to be improved, it is also important to accept that failure (including hijacking, unauthorised access) remain possible and reliance on systems should remain at acceptable levels, and recovery actions need to be designed in.

**Automatic Updates and Patching:** Devices should support remote, secure firmware updates (OTA) to address security vulnerabilities and improve performance without downtime. Organizations should establish clear policies for managing software lifecycles – including having a clear understanding of responsibility/liability if things go wrong under specific circumstances.

**DDoS Mitigation Strategies:** IoT networks should employ rate limiting, anomaly detection, and AI-based filtering to limit the prevalence and severity of distributed denial-of-service (DDoS) attacks. Protective measures should be regularly reviewed and updated to counter evolving threats.

**Disaster Recovery and Incident Response:** Developing a comprehensive incident response plan, including backup and disaster recovery strategies that take data protection necessities and legislation into account and ensures quick recovery from failures. Regular security audits should be conducted to validate compliance.

**Impact of AI and Quantum Computing:** AI can improve system resilience by predicting failures and dynamically allocating resources to prevent disruptions

### 4. Usability and Interoperability

**User-Centered Design:** IoT interfaces should prioritize ease of use, accessibility, and clear feedback mechanisms to enhance user experience as well as users' ability to take effective security measures. Ethical AI should try to ensure decision-making is explainable and free from bias.

**Standardized Protocols and APIs:** Adhering to open standards can enhance interoperability among IoT systems, reducing vendor lock-in..

**Lifecycle Management:** Devices should have defined support lifecycles, including software updates and end-of-life policies to ensure longevity and sustainability. Manufacturers should be made responsible for ensuring waste disposal and material use from the design phase onward.

**Impact of AI and Quantum Computing:** AI-powered automation can enhance usability by enabling adaptive interfaces and intelligent assistance for IoT users – but also for

abusers. Quantum computing has the potential to optimize IoT network efficiency, reducing latency and improving processing speeds, thus potentially enhancing interoperability and system-wide coordination.

## **5. Ethical and Sustainable IoT**

**Energy Efficiency:** Implementing low-power IoT designs, such as LPWAN and energy harvesting techniques, reduces environmental impact. IoT deployments should minimize carbon footprints and promote responsible energy consumption – even more so in the understanding that IoT deployment continues to increase towards the future.

**Ethical AI and Decision-Making:** IoT-driven AI should be transparent, explainable, and free from bias to ensure fair decision-making in critical applications. AI must respect human rights and reflect global ethical standards in IoT governance.

**Human Oversight:** Automated systems should include human intervention mechanisms to avoid unintended consequences in high-stakes environments. Justifiable trust must be established through ethical principles and accountability measures.

**Impact of AI and Quantum Computing:** AI can contribute to sustainable IoT by optimizing energy consumption and reducing waste through predictive analytics. Quantum computing may revolutionize material science and energy storage, enabling more sustainable IoT hardware. However, ethical considerations must guide these advancements to prevent unintended consequences such as bias, inequality, or environmental harm. And it will be necessary to agree on measuring this to ensure accountability.

### **Future Outlook**

As AI and quantum computing continue to advance, they will play a transformative role in shaping IoT ecosystems. AI-driven automation and predictive analytics will enhance IoT usability, security, and resilience, while quantum computing will enable new levels of computational efficiency and encryption. However, organizations must proactively address the risks associated with these technologies, including ethical concerns, cybersecurity threats, and potential disruptions to current security frameworks. A collaborative approach involving policymakers, industry leaders, and researchers is essential to ensure that IoT development remains secure, ethical, and sustainable for future generations.

---

*For suggestions, questions and remarks please reach out to Maarten Botterman, Chair of IGF DC IoT.*