# Joint INGAA & INGAA Foundation Cybersecurity Commitments



**In recognition that cybersecurity is a shared responsibility, INGAA members and INGAA Foundation members jointly agree to maintain foundational cybersecurity practices that support the protection of information and enable timely coordination during security events.**

## 1. Security Point of Contact

Operators and service providers designate and maintain a primary cybersecurity or security contact responsible for coordinating security matters with the other, including vulnerability reports and security incident communications.

## 2. Security Incident Notification

Operators and service providers directly notify the other party's designated cybersecurity contact of any confirmed or reasonably suspected cybersecurity incident that may affect the other party's data, systems, or services.

Notification will be provided within 72 hours of discovery and will include relevant details known at the time, with updates provided as additional information becomes available.

## 3. Protection of Information

Operators and service providers implement reasonable administrative, technical, and physical safeguards to protect operator and service provider information from unauthorized access, disclosure, alteration, or destruction.

Upon request or termination of services, operators and service providers will return or securely destroy any information in their possession unless retention is required by law.

These safeguards should be appropriate to the size of the operator and service provider, the nature of the services provided, and the sensitivity of the information involved.

## 4. Vulnerability and Security Issue Cooperation

Operators and service providers agree to reasonably cooperate with one another in the investigation and remediation of security vulnerabilities or risks related to any products or services that may affect the operators or service providers.

This may include coordination regarding security updates, mitigations, or other reasonable remediation actions.






### 5. Cybersecurity Assessments & Audits

Operators and service providers each conduct periodic internal cybersecurity audits and risk assessments consistent with industry standards and applicable legal and regulatory requirements. Such audits evaluate the effectiveness of administrative, technical, and physical safeguards designed to protect information and systems from unauthorized access, disruption, modification, or disclosure. Each party maintains documentation of material audit findings and remediation efforts.

### 6. Multi-Factor Authentication

Operators and service providers use multi-factor authentication (MFA) where available for accounts used to access the other party's systems, environments, or sensitive information.

### 7. Patching

Operators and service providers apply appropriate security updates or patches to systems, applications, or devices used to provide services to the other party within a reasonable timeframe.

### 8. Least Privileged Access

Service providers will limit access to operator systems or information to personnel with a legitimate business need and will promptly remove access when no longer required.

### 9. Employee Screening

Operators and service providers will ensure personnel assigned to provide services to one another are subject to appropriate background screening and confidentiality obligations as permitted by applicable law.

### 10. Cybersecurity Training

Operators and service providers maintain a cybersecurity awareness and training program for all employees, including more specialized training for personnel with access to data, systems, or services of the other party. Such training is provided upon hire or engagement and periodically thereafter, and addresses cybersecurity risks, security responsibilities, incident reporting procedures, and the protection of sensitive information.

Operators and service providers each conduct periodic phishing testing for all employees. Employees failing a phishing test are required to complete targeted follow-up cybersecurity training.

### 11. Subcontractor Security Responsibilities

If the service provider uses subcontractors or third parties in the delivery of services to the operator, the service provider will ensure such parties are bound by confidentiality and security obligations that are no less protective than those required of the service provider with respect to operator information.




