UIAA Data Breach Response Procedure

Preparation Phase:

a. Establish a Response Team: Designate a cross-functional team comprising representatives from IT, legal, communications, anti-doping, and management.

b. Identify Relevant Regulations: Ensure familiarity with relevant data protection laws, anti-doping regulations, and IF anti-doping rules.

c. Conduct a Risk Assessment: Assess potential data breach risks associated with anti-doping activities, including sensitive athlete information and test results.

Detection and Containment:

a. Early Detection: Implement protocols to detect potential data breaches promptly.

b. Containment Measures: Upon detection, immediately isolate affected systems or data to prevent further exposure.

Assessment and Investigation:

a. Formal Investigation: Initiate a thorough investigation to determine the cause, scope, and impact of the data breach.

b. Gather Evidence: Collect and preserve evidence related to the breach, ensuring compliance with legal and regulatory requirements.

Notification and Communication:

a. Internal Notification: Inform the response team and key stakeholders within the IF about the breach.

b. External Notification: Notify relevant authorities, such as WADA, anti-doping agencies, regulatory bodies, and affected individuals, in accordance with applicable laws and regulations.

c. Public Communication: Develop and disseminate a clear and transparent communication plan to address media inquiries and reassure stakeholders, where needed.

Remediation and Recovery:

a. Mitigation Measures: Take immediate steps to mitigate the impact of the breach, such as enhancing security measures and implementing additional safeguards.

b. Support Affected Individuals: Provide support and assistance to affected athletes, officials, and other stakeholders, including access to counseling or legal resources if necessary.

c. Data Restoration: Restore affected data from backups or other sources as necessary, ensuring data integrity and confidentiality.

Evaluation and Learning:

a. Post-Incident Review: Conduct a comprehensive review of the incident response process to identify strengths, weaknesses, and areas for improvement.

b. Update Procedures: Incorporate lessons learned from the data breach into the response procedure, making necessary revisions to enhance future preparedness and resilience.

Documentation and Reporting:

a. Document Incident Details: Maintain detailed records of the data breach, including timelines, actions taken, and outcomes.

b. Regulatory Reporting: Comply with any legal or regulatory requirements regarding data breach reporting, including notifications to relevant authorities and regulatory bodies.

Training and Awareness:

a. Employee Training: Provide regular training and awareness programs for IF employees to educate them on data protection best practices and their roles in responding to data breaches.

b. Simulation Exercises: Conduct periodic tabletop exercises and simulations to test the effectiveness of the response procedure and ensure readiness for real-world incidents.

By following this Data Breach Response Procedure, the IF can effectively respond to data breaches related to anti-doping matters while minimizing the impact on athletes, officials, and organizational reputation.