情報セキュリティ規程

第 1 章　総則

第 1 条（目的）

本規程は、一般社団法人全日本大学ソフトボール連盟（以下「本連盟」という。）が保有する情報資産の機密性、完全性及び可用性を維持し、情報漏洩、改ざん、紛失等の事故を未然に防止することを目的とする。

第 2 条（用語の定義）

本規程において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

1. **情報資産：** 本連盟が業務上保有する全ての情報（紙媒体、電子データ）及びそれを取り扱う情報システム、ネットワーク機器、記録媒体。
2. **機密性：** 許可された者だけが情報にアクセスできること。
3. **完全性：** 情報が正確かつ最新の状態に保たれ、不正に改ざんされないこと。
4. **可用性：** 必要になったときに、いつでも情報にアクセスできること。

第 3 条（適用範囲）

本規程は、本連盟の全ての役員、職員、及び本連盟の業務に従事する者（委託先を含む）に適用する。

第 2 章　管理体制

第 4 条（情報セキュリティ管理責任者）

1. 本連盟に「情報セキュリティ管理責任者」を置き、事務局長（またはシステム担当理事等）をもって充てる。
2. 管理責任者は、情報セキュリティ対策の策定、実施、及び教育を統括する。

第 5 条（構成員の義務）

構成員は、本規程及び関連する法令を遵守し、情報資産の適切な取扱いに努めなければならない。

第 3 章　情報資産の取扱い

第 6 条（情報の格付けと管理）

情報セキュリティ管理責任者は、情報資産の重要度に応じて格付けを行い、アクセス権限の設定や保管場所の指定を行う。特に選手名簿や財務情報等の機密性の高い情報は厳重に管理しなければならない。

第 7 条（PC・記録媒体の管理）

1. 業務に使用する PC、タブレット、スマートフォンには、パスワードまたは生体認証を設定しなければならない。
2. 個人所有のデバイスを業務に利用（BYOD）する場合は、管理責任者の許可を必要とし、セキュリティ対策が講じられていることを確認しなければならない。
3. 選手名簿等の重要データを含む USB メモリ等の持ち出しは原則禁止とし、やむを得ない場合はデータを暗号化するなど、適切な対応を必須とする。

第 8 条（パスワード等の管理）

構成員は、業務で使用するアカウントのパスワードを適切に管理し、他者への漏洩や使い回しを避け、定期的に変更するよう努めなければならない。

第 4 章　ネットワーク及びシステム管理

第 9 条（ウイルス対策）

本連盟が管理する PC 等の端末には、必ずウイルス対策ソフトを導入し、常に最新の状態に更新しなければならない。

第 10 条（SNS および外部サービスの利用）

1. 本連盟の公式 SNS アカウントの管理者は、管理責任者が指名する。
2. 構成員は、SNS において本連盟の未公開情報、守秘義務のある事項、または個人の名誉を傷つける内容を投稿してはならない。
3. クラウドストレージ等の外部サービスを利用する場合は、安全性が確認されたサービスに限定する。

第 5 章　事故対応及び教育

第 11 条（事故発生時の報告）

構成員は、情報資産の紛失、盗難、漏洩、ウイルス感染等の事故が発生した、またはその疑いがあることを知ったときは、直ちに管理責任者に報告しなければならない。

第 12 条（緊急措置と再発防止）

管理責任者は、事故報告を受けた場合、速やかに被害拡大を防止するための措置を講じ、原因究明を行い、理事会に報告するとともに再発防止策を策定する。

第 13 条（教育）

本連盟は、役員および職員に対し、情報セキュリティ意識の向上を図るため、定期的に教育・訓練を実施する。

第 6 章 附則

第 14 条(改定)

本規程の改定は、理事会の決議によらなければならない。

第 15 条(施行期日)

本規程は、2026 年 6 月 27 日から施行する。