製品サイバーセキュリティ脆弱性管理ポリシー

(A) 概要

明曜科技股份有限公司 (以下「当社」といいます) は、潜在的なサイバーセキュリティリスクへ迅速に対応できるよう、包括的かつ効率的な製品セキュリティ脆弱性対応体制の構築に努めています。

当社は、製品におけるサイバーセキュリティリスクを低減するため、信頼性の高い技術ガイダンスおよび解決策 (または緩和策) を継続的に提供します。

当社 PSIRT (Product Security Incident Response Team) は、国際的な法規制および標準に基づき、脆弱性対応プロセスおよび対策を策定・管理し、関連する運用体制の有効性を確保します。

本ポリシーを通じて、当社従業員が統一された明確な方法でサイバーセキュリティ問題へ対応し、関連する対応フローを理解できるようにします。

(B) 適用範囲

本ポリシーは以下に適用されます。

- 当社のすべての製品

  （蓄電システム、バッテリーマネジメントシステム（BMS）および関連設備を含みますが、これらに限定されません）

- 当社へ報告されたすべてのサイバーセキュリティ脆弱性案件

標準製品以外の製品またはカスタマイズ製品については、双方間の契約または別途合意された条件に従って対応します。

(C) サイバーセキュリティ脆弱性の報告方法

当社製品にサイバーセキュリティ上の脆弱性が存在する可能性を発見された場合は、以下の方法にてご報告ください。

- 電子メール： service@eticabattery.com
- 公式ウェブサイト： https://etica.tw/contact-us/

当社は、提出されたすべての脆弱性報告を確認し、必要に応じて報告者へ連絡いたします。

なお、情報が不完全、不正確、重複、または明らかに虚偽である場合、当社は対応を行わない権利を有します。

問題分析および対応を円滑に行うため、以下の情報をご提供いただくことを推奨します。

- 製品種類
- 製品名称
- ソフトウェア / ファームウェアのバージョン
- 脆弱性の詳細説明
- 再現手順

善意通報原則善意による報告原則

当社は、善意によるサイバーセキュリティ脆弱性の報告を推奨しています。

本ポリシーに基づく善意の研究および報告行為について、システム破壊や情報漏えいを伴わない限り、当社は原則として法的責任を追及しません。

(D) 製品サイバーセキュリティ脆弱性管理プロセス

当社の脆弱性管理プロセスは、以下の 5 段階で構成されます。

1. 報告受理確認（原則として 2 営業日以内に返信）
2. 選別および初期分析

3. 調査分析（開発チームと連携）
4. 修正および緩和策の実施
5. 情報公開（必要に応じて実施）

(E)脆弱性の深刻度および影響評価

当社は、CVSS（Common Vulnerability Scoring System）に基づきリスク評価を行います。

レベル	CVSS 3.x スコア
Critical（重大）	9.0 – 10.0
High（高）	7.0 – 8.9
Medium（中）	4.0 – 6.9
Low（低）	0 – 3.9

(F) 免責事項

本ポリシーの内容は、予告なく変更される場合があります。

当社は、すべての報告案件に対して回答または解決策を提供することを保証するものではありません。

本文書の利用に伴うリスクは、利用者自身の責任において負担するもの

とします。