タイプ： サイバー ターゲット：すべて	緊急時に従うべき手順を示した書面 **ランサムウェア－ークステーションの大規模な使用不能**	

1. アラート

しない	する
何も削除しない：すべての情報は調査の証拠として使用されます	セキュリティ・オペレーション・センター（SOC）と情報システム・セキュリティ・マネージャーにアラートを出す
暗号化されたファイルやアプリケーションを開かない：感染を止めなければなりません	攻撃の規模と緊急対応の優先順位を評価するため、すべての情報を SOC と共有する
	SOCの指示に従う

2. 緊急時の対応

1. 重要なシステムを分離する：
   - すべてのネットワークを切断する
   - コンピュータからネットワークケーブルを外す
   - Wifi接続を切断する
2. すべての周辺機器を外す
3. 侵害の規模を評価し、証拠を収集する

3. 継続のための解決策

業務の重要度順に、どのワークステーションからでもインターネット経由でアクセスできる仮想化された作業環境の提供

4. 事業継続 計画 の発動基準

危機管理部門が BCP (ビジネス継続プラン) 発動の最終決定を行う
基準1：ワークステーションの5%が使用不能
基準2：ランサムウェアが他のサイト/エンティティ/アプリケーションに広がるリスク