筑紫野市立小中学校校務系環境更新事業

仕様書

筑紫野市　学校教育課

対象範囲

1.1. 本調達の範囲

以下に、本調達範囲を記載する。

項目		説明
ネットワーク統合		
	ネットワーク統合	新校務端末は、GIGA 系ネットワークに接続する。新校務端末から既存プリンタへの印刷を許可するための、ネットワーク機器（ルータ等）設定変更等は別契約にて既存業者が実施することとする。
ゼロトラスト型システム基盤		
	ID 統制	ID 管理基盤、多要素認証、SSO、アクセスコントロール等
	デバイス統制・保護	機能制限、紛失時対応、リモートアクセス、ポリシー等一斉配布、Windows Update 等一斉管理、IDaaS との連携等
	EPP	マルウェア検知・遮断等
	EDR	SOC 等による監視機能、攻撃後の対応、IDaaS との連携等
	ネットワークセキュリティ	アプリケーション単位の接続制御、IDaaS との連携、通信経路の暗号化、悪性な WEB コンテンツへのアクセス制限（フィルタリング）、WEB 経由データのマルウェア検出、シャドーIT の制限、テナント識別等
	データ漏えい防止	機密ファイルやメールの暗号化及びアクセス制御等
	ログの収集・分析	校務端末のログ収集、可視化
	クラウドストレージ及びバックアップ構築	機密性の高いデータの保存場所と想定しており、業務継続性を確保するために迅速なデータ復旧が行えるよう、別途随時バックアップを取得する構成とする必要があると考えている。
校務用端末調達		
	校務用端末本体の調達	メーカーからの調達、納期調整
	校務用端末のキッティング及び搬入設置	新しい校務用端末の初期設定、キッティング、設置・移行に係る対応
	校務用端末の保守	ハードウェア等の保守（一次切り分け、障害対応）

なお、校務支援システムについてはふくおか電子自治体共同運営協議会が構築を進めている統合型校務支援システムを令和 7 年 4 月より利用予定である。

システム構成

2.1. 本事業の考え方

本市においては、ふくおか電子自治体共同運営協議会が構築を進めている統合型校務支援システム（以下、校務支援システムという。）を、令和７年度から利用することを予定しています。当該システムの利用に際して、本市はデータ管理及びセキュリティに課題を抱えており、文部科学省が発出した「教育情報セキュリティポリシーに関するガイドライン（令和６年１月)」で示す「アクセス制御による対策を講じたシステム構成」を構築することにより、校務支援システムへのセキュアな接続環境を整備するとともに、データ管理及びセキュリティの観点から将来を見込んだ先進性を備え、長期間にわたって安心かつ安全に教職員が勤務できる環境整備を目指します。

本事業においては下記の項目を重視しています。

①校務系の ID 管理の一元化

②学校外での業務を見越したクラウドサービス基盤による利便性の向上

③情報漏えい防止のためのデータ管理・制御

④ディレクトリサービスによるユーザー保守・管理負担の軽減

・前述の本事業の考え方に基づき本市で検討を重ねた結果、Microsoft 365 が持つサービスおよび機能を活用することを想定しているが、別ソリューションの提案を行う場合は、後述する要件を満たすソリューションであると共に、有効性・コスト・運用面のメリットについて提案をすること。

・要求機能に掲げる事項のみを実現すればよいのではなく、全体が機能するために当然実現しなければならない機能・作業も含まれるものとし、高価・複雑・不安定よりも安価・単純・頑丈なシステムの構築を目指すこと。

・最新あるいは今後リリース予定のサーバ OS、クライアント OS、ブラウザのバージョンにも対応できるよう考慮されたものとすること。

・クライアントは DHCP での運用を基本とする。

・セットアップ等の作業場所は受注者側で確保すること。ただし、システム基盤構築作業の接続を要するものについては、作業場所を協議の上で決定することとする。その場合において、市側で大規模な作業場所を確保することは困難な為、留意の上で見積および作業を行うこと。

・今回構築する環境に切り替える際、既存環境を長期間停止することは業務への支障が大きいため、停止期間等の影響が最小限となるよう考慮すること。

・令和 7 年１月から校務支援システムの仮稼働、および令和 7 年４月から校務支援システムの本稼働を開始できるよう各種の構築を行うこととする。

システム基盤の機能要件

本システムは筑紫野市で稼働している Microsoft365 テナント上に構築することを想定している。新たなシステムの構築による既存環境への影響が無いことに十分考慮して下記機能を実装すること。また、各種サービスの提供に必要なライセンス数は本調達に含めること。

・教職員等数：694 人、校務用端末台数総数：709 台（うち予備機 15 台）

3.1. ゼロトラスト型システム基盤要件

3.1.1. 認証基盤

当システムについては、「Microsoft Entra ID」を利用することを想定している。なお、以下の要件を満たす同等の代替サービスによる提案も可とする。

・サービスを利用するためにサーバの設置や Agent インストールを必要とせず、Windows、Mac、iOS、Android 等様々な OS に対応し、特定のデバイスに依存しない認証サービスを利用できること。
なお、Authenticator など認証アプリケーションのインストールは可能とする。
・主要な機能をブラウザで管理できること。また、特殊な機能の設定や一括処理をする際には PowerShell や API を使ったプログラム等からの管理ができること。
・今回調達する校務端末及び再利用端末について、校務システムにアクセスできるよう構築を行うこと。
・ユーザー、ユーザーの所属するグループ、接続元ネットワークの IP アドレスや、接続するデバイスの状態に応じてサービスの利用できるように構築をおこなうこと。
・パスワードのリセットや再発行等のアカウント管理手法について具体的な提案を行うこと。
・管理者は利用者の認証アクセス状況をレポートとして確認することができるとともに、外部からの不正アクセスの疑いのある事象についての対処方法、アカウントのセキュリティ対策についても具体的な提案を行うこと。
・ふくおか電子自治体共同運営協議会が構築を進めている統合型校務支援システムへのユーザー認証・連携を考慮に入れた設計構築をおこなうこと。
また、校務支援システムの Web アプリケーションに対して、外部からの安全なリモートアクセスを可能とするための機能を有していること。
・人事異動・組織改変に対して、柔軟かつ簡単に対応できるよう考慮すること。
・学習 e ポータル、業務にて利用するサービスとのユーザー情報連携が可能であること。

3.1.2. メールシステム

当システムについては、「Exchange Online」を利用することを想定している。なお、以下の要件を満たす同等の代替サービスによる提案も可とする。

（1）メールシステム

・構築するネットワークの内外に対してメールの送受信が行えること。

・現行利用しているメールアドレス、ドメインを新環境でも利用できること

・個人のメールアドレスとは別に学校代表アカウント、共有メールアドレスの設定を行えるようにすること

（2）メールセキュリティ対策機能

・メールによる標的型攻撃等の高度な脅威からの保護を目的として、危険な添付ファイルに対する対策と、悪意のあるリンクに対する保護を実施できること。

・ゼロデイ攻撃等未知の攻撃手法に対しても可能な限り添付ファイルの安全性を検証するため、サンドボックス環境等により動的解析を実施したうえで受信できる機能を有すること。

・既知の攻撃に対してはメールボックスに届く前に安全性を精査すること。また、ゼロデイ攻撃等未知の攻撃に対しては端末の EDR 等により添付ファイルの安全性を分析する機能を有すること。

・メール本文中の URL やハイパーリンクについて、リンク先の安全性についてチェックできること。また、当該リンク先がファイルであった場合は、添付ファイルと同様にサンドボックスでスキャンできること。

・メール本文中の URL やハイパーリンクについて、不審なものである場合、利用者がクリックした際に適切な処置ができること。

・脅威を検知したメールの状況・統計情報・アクション(配送、隔離、削除等)等が確認できること。

3.1.3. ファイル共有システム

当システムについては、「Share Point Online」を利用することを想定している。なお、以下の要件を満たす同等の代替サービスによる提案も可とする。

・共同作業や情報を共有する利用者を指定したチームを作成でき、チーム内限定のビジネスチャットやファイル共有等が行えること。

・チーム内に目的に応じたチャネルを作成でき、ビジネスチャットやファイル共有を整理して行えること。

・「ファイル共有・管理」サービスと連携し、ファイルの共有や Office ファイルの共同編集機能を提供すること。

・ファイルのアップロードやダウンロード、閲覧、編集において可能な限り統合コミュニケーションサ

ービスのアプリケーション内で操作が完結すること。
・認証基盤に登録されたユーザー及びグループ毎にセキュリティ、アクセス権等が設定できること。
・後述するセキュリティ要件を満たすよう、アカウント属性に対応したラベル設定に応じて、各ファイルの暗号化が可能であること。
・ファイル共有システム内で、削除、紛失、破損等のよる要因で使用できなくなったファイルを復元する機能を有すること。
・現行のファイルサーバ資産を新サービスへ移行すること。
・(現行ファイルサーバ資産容量：各校約 2TB 程度) ファイルサーバ資産移行に際し、当システム内のチャネル階層の構成、セキュリティ設定等は、現行ファイルサーバに準拠したものとし、移行タイミングにおける利用者の負担を極力軽減するように努めること。
・移行についてはダウンタイムが発生しないように新ファイルサーバへの移行を行えるよう提案すること。
・データ移行の方法については契約後、別途協議のうえ決定すること。

3.1.4. グループウェア

当システムについては、「Teams」を利用することを想定している。なお、以下の要件を満たす同等の代替サービスによる提案も可とする。

・PC より、電子メール、チャット、音声、動画、資料共有等を用いたコミュニケーション機能を提供すること。なお、音声通話機能、ビジネスチャット機能及び Web 会議機能を、原則として単一のツールにより提供すること。
・外部関係者とのコミュニケーションにも使用できること。
・外部関係者とのやりとりについてはセキュリティに配慮した設計を行うこと。
・任意の複数の利用者とテキストメッセージ（チャット等)、音声、ビデオ、ファイル及び画面共有を用いたリアルタイムの会議（以下 Web 会議）ができること。
・専用クライアントアプリケーション以外に、ブラウザーベースのクライアントで主要機能が利用できること。
・共有されたファイルに対し、複数メンバーでのリアルタイム同時編集が可能であること。
・管理者によって保持ポリシーを設定でき、一定期間保持する、一定期間経過後削除するといった制御が可能なこと。

3.1.5. EPP および EDR

・Windows 11 に対する侵入検知などのログ情報を収集し、世界中のセキュリティインシデントデータと照らしあわすことにより異常な挙動や攻撃者の手法を検出し管理ポータルから一元的に管理、確認

可能であること。

・端末のふるまいを検知して脅威の検出を行うこと
・各端末の脆弱性情報を確認することができること
・検出した脅威を可能な限りリモートで除去することができること。
・脅威が検出された端末を管理ポータルの操作により遠隔でネットワークから隔離できること。
・脅威の侵入経路などのトラッキングが行えること。
・定期的に最新のセキュリティ状態に更新がされること。

3.1.6. 資産管理システム

当システムについては、Microsoft 365 に含まれる MDM「Microsoft Intune」と「SKYSEA ClientView」を資産管理システムとして利用することを想定している。なお、以下の要件を満たす同等の代替サービスによる提案も可とする。

・OS として、Windows、iOS、Android を使用するデバイスについて各デバイスの設定を強制する機能を有すること。
・OS として、Windows、iOS、Android を使用するデバイスについてデバイスを初期化することができること。
・MDM にデバイス登録することで、登録済みデバイスのみアクセスを許可する設定ができること
・Windows 機能更新プログラムのバージョン固定等の更新プログラム管理ができること。
・管理画面から、ログの閲覧、資産情報の閲覧、USB メモリの管理、ポリシーの適用、ソフトウェア配布等が可能なこと。
・各クライアントコンピューターに関する各種ハードウェア情報を、資産情報として自動的に収集できること。
・収集したハードウェアおよびソフトウェア情報を、一覧で表示できること。
・指定したクライアントコンピューターに対して、任意のプログラムを配布し、自動的にプログラムのインストールおよびアンインストールを行う機能を有すること。
・配布したソフトウェアの配布状況およびインストール状況を確認することができること。配布したソフトウェアのインストール / アンインストールが失敗した場合は、失敗したクライアントコンピューターを指定して再実行が行えること。
・クライアントコンピューターがソフトウェアの配布を受ける際、すでに同一のセグメント内のクライアントコンピューターに配布されたソフトウェアがキャッシュとして残っている場合、そのクライアントコンピューター（以下キャッシュ端末と呼ぶ）からソフトウェアを配布できること。
・4GB 以上のサイズのソフトウェアをキャッシュ配布で配布できること。
・指定したクライアントコンピューターに対して、Windows 更新プログラムを配布し、自動的に更新プログラムの実行を行う等のセキュリティパッチを適用する機能を有すること。

・配布した Windows 更新プログラムが適用されていないクライアントコンピューターを検出し、一覧化できること。
・クライアントコンピューター上で印刷が実行された際に、その印刷されたドキュメント名、１回の印刷枚数、ファイルパスなどをログとして記録できること。
・クライアントコンピューターから One Drive へのアップロードおよびダウンロード操作に対して、ログを収集できること。
・また、アップロード元およびダウンロード先ファイルのフルパスを記録できること。
・ルールに反した操作をしたクライアントコンピューターの利用者に注意を促すため、メッセージの内容はルール違反の操作ごとに設定できること。
・指定したアプリケーションの実行を検知および禁止できること。
・クライアントコンピュータ上での、Web サイトの閲覧や Web サイトからのファイルダウンロード／アップロード操作を検知及び禁止できること。ただし、フィルタリング等の他製品で仕様を満たすことも可とする。
・Web サイトの閲覧や Web サイトからのファイルアップロードを禁止する際は、キーワードや URL で禁止サイトを設定できること。
・特定の URL からのダウンロードを禁止から除外するよう、設定できること。ただし、フィルタリング等の他製品で仕様を満たすことも可とする。
・USB デバイス台帳に登録されたデバイス情報を基に、その USB デバイスの使用許可/不許可などを設定できること。
・許可した USB デバイスのみを使用可能としそれ以外の使用を禁止できるような運用が可能であること。
・個々の USB デバイスに使用可能/読み取り専用/使用不可能を設定できること。
・デバイス種別ごとに、一括で使用可能/読み取り専用/使用不可能の設定ができること。
・設定ができるデバイスの種類は以下の通りとする。
・デバイス種別：USB メモリ、USB ハードディスク、CD/DVD ドライブ、Blu-ray ドライブ、デジタルカメラ、モバイル端末、USB デバイスや CD/DVD/Blu-ray ドライブなどの記憶媒体を、クライアントコンピューターに接続したり、書き込みを行った場合に検知および禁止ができること。

3.1.7. フィルタリング

・安全な Web サイトにのみアクセスできるホワイト運用又はブラックリスト運用が可能な DB を搭載していること。
・ファイルの拡張子をリスク別にダウンロード制限が可能であり、Web サイトにアクセスしただけでマルウェアに感染してしまう攻撃の対策ができること。
・なお、OS やアプリケーションのアップデートなどに利用されるサイトのダウンロードは許可でき、利便性を損なわずにセキュリティを担保できること。

・フィルタリング設定のテンプレートが用意されていること。また、日本の組織に応じたグループ・ユーザー管理ができそれを基にフィルタリグルールの設定ができること。
・国内で販売されている製品で、日本語によるサポート対応が可能であること
・レポート機能が無償で付属されており、外部 DB を用意せず利用可能なこと。
・グループごとに有効期間が指定でき、特定日以降フィルタリング開始とするグループ事前設定や、複数のユーザーおよびグループを対象にする柔軟なポリシー作成が可能なこと。また、ユーザーの Web 利用のフィルタリング機能の時間制限ができること。
・脅威情報への通信が発生した際に、管理者にメール通知が可能なこと。
・脅威情報サイトへのアクセス情報（アクセスの発生日時、該当ユーザー、該当端末、適切な対処方法）に関するレポートを管理者にて確認することが可能なこと。

3.1.8. 多要素認証

当システムについては、「Windows Hello」を利用することを想定している。
・ログイン方法は Windows ログオンによるものとし、顔認証、PIN コードによる二要素認証に対応していること。
・前述の認証基盤と連携することとし、認証基盤の登録情報を元に認証するものとする。
・ネットワーク障害によりクライアントがネットワークから切り離された場合、キャッシュ等により一定期間内はクライアントにログインできること。
・生体情報の読み込みが正常にできない場合に、他の方法を用いてログオンが可能なこと。

システム基盤の非機能要件

4.1. 規模・性能要件

利用者数・データ量に応じた、経済的かつ高パフォーマンスなシステム導入のため、規模・性能要件は、次のとおりとする。

本システムを利用する端末は、次のとおりである。サーバ機器およびサービスの選定では、これを踏まえて、快適な使用環境が実現されるよう最適な機器・サービスのサイジングを行うこと。

＜規模について＞

校務系	・校務用端末 … 715 台(うち、607 台を新規調達し、108 台は既存端末を再利用する。 ※詳細仕様に関しては 5. 校務用端末の機能要件を参照すること。 また、別添①「校務端末配置計画表」を参照すること。

4.2. セキュリティ要件

4.2.1. 教育情報セキュリティポリシーに関するガイドラインへの準拠

・令和 6 年 1 月に改訂された教育セキュリティポリシーに関するガイドラインに準拠すること。

4.2.2. 認証とアクセス制御

・校務系端末と Microsoft 365 サービスのシングルサインオンを行うこと。
・端末へのサインインについては、2 要素以上の多要素認証を行うこと。
・テレワーク等で外部から校務支援システムへアクセスする場合は、校務端末からの接続のみ許可するようにアクセス制御を行うこと。
・テレワークの際にはモバイルデバイス等を使った多要素認証が可能であること。本要件については必須とはしないが、導入時の設計・テストにおいて利便性を考慮した上で採用を検討すること。
・校務支援システムに接続する際には、Microsoft365 で認証された特定の端末及び特定のユーザーからのみの接続を許可すること。

4.2.3. 情報漏洩対策

・教職員が新規作成・編集したファイルは教職員しか閲覧することができない機密ラベルを付与すること。
・教職員が新規作成・編集時に付与する機密ラベルのレベルの変更（役職に応じた閲覧・編集範囲の制限など）が可能で、レベルの詳細については設計にて定義すること。
・なお、児童生徒などとファイルを共有するための機密ラベルを解除の方法については、役職者に限定するなど柔軟な設定が可能なこと
・メールの誤送信があった場合でもアクセス権のない者が閲覧できないように対策できること。

4.2.4. ログの保管

・以下に記載するログ管理を行えるように構築すること。
Microsoft 365 サービスのアクティビティログ
  - Entra ID のサインインログ
  - Entra ID の監査ログ

・ログはクラウド上で統合管理し、脅威の分析・可視化を可能とすること。
・認証基盤と連携して管理ポータルへのアクセス制御を行うこと。
・クライアントコンピューターに対して行われた操作、ログオン・ログオフの日時、ファイル操作、Web へのアクセスおよびアップロード・ダウンロード、USB メモリなどの記憶媒体を利用した内容、記憶媒体のシリアル情報等をログとして記録する機能を有すること。

・Web サイトの閲覧が行われた内容について、ウインドウタイトル、URL をログとして記録できること。また、Web ダウンロードおよび Web サイトへの書き込みが行われた内容について、URL、書き込み内容などをログとして記録できること。尚、以下のブラウザに対応していること。
Google Chrome、Microsoft Edge (Chromium 版)、Firefox
・クライアントコンピューター内の蓄積されたログ（一時的なログを含む）については、暗号化等により保護され、クライアントコンピューター利用者はログの内容を確認できない機能を有すること。

4.2.5. セキュリティソフト・セキュリティパッチの要件

・Windows の校務端末に対しては、品質更新プログラムを随時配信すること。なお、意図していないタイミングで配信されないよう、予めスケジュールの設定が可能であること。
・Windows の機能更新プログラムについては、バージョン固定等が可能であること。
・機能更新を行う場合は事前にテスト端末等で更新後の挙動を確認した上で配信を行うこと。
・校務端末に関してはユーザー操作により更新処理を実行できるようにすること。なお、テレワーク時でも更新が可能となるよう可能な限りインターネット経由で配信すること。
・校務端末の更新プログラムの適用状況を確認できる仕組みを構築すること。

校務用端末の機能要件

5.1.1. 設置台数一覧

	名 称	利用者数	設置台数 （新規端末）	設置台数 （再利用端末）
1	筑紫野市教育委員会	2	2	0
2	二日市小学校	５６	４８	8
3	二日市東小学校	６７	５９	8
4	吉木小学校	３０	２５	5
5	阿志岐小学校	２３	１８	5
6	山家小学校	２２	１７	5
7	筑紫小学校	７２	６４	8
8	山口小学校	２９	２３	6
9	二日市北小学校	３９	３４	5

10	原田小学校	４７	４１	6
11	筑紫東小学校	３８	３３	5
12	天拝小学校	３０	２４	6
13	二日市中学校	５９	５１	8
14	筑山中学校	５１	４４	7
15	筑紫野中学校	５１	４３	8
16	天拝中学校	３０	２４	6
17	筑紫野南中学校	４８	４１	7
18	予備機		１６	5

5.1.2 ハードウェア仕様

項目	仕様	特記事項
機種タイプ	ノート PC としてもタブレットとしても使用できる 2in1 タイプ（コンバーチブル型又はデタッチャブル型）の機種であること。	
筐体	13.3 型以上ワイド液晶モデル 解像度： Full HD (1920×1080)以上 タッチパネル式	
OS	Windows11 Pro (64bit)	
CPU	インテル® Core™ i5 プロセッサー (HT テクノロジー対応) 第 12 世代以上	
メモリ	16GB 以上	
ストレージ	SSD256GB 以上	
インターフェース	USB2.0 以上 1 ポート以上、USB3.2 以上 1 ポート以上 HDMI×1 以上 LAN コネクタ×1 (RJ-45) (変換アダプタによる対応も可とする) φ3.5mm ステレオ・ミニジャック (マイク・ラインイン・ヘッドホン・ラインアウト・ヘッドセット兼用端子)	
ネットワーク機能	LAN (1000BASE-T/100BASE-TX/10BASE-T 対応) 内臓無線 LAN (IEEE802.11 a/b/g/n/ac/ax)	
オーディオ機能	スピーカー及びマイク内蔵	
キーボード	日本語キーボード、JIS 配列準拠	
バッテリー	リチウムイオン バッテリー駆動 10 時間以上	

	※バッテリー駆動時間は JEITA バッテリー動作時間測定法（Ver. 2.0）による測定値とする。	
重量	1.5kg 以下	
Web カメラ	フロント内蔵（有効画素数約 92 万画素、Windows Hello 対応）以上	
付属品	光学式マウス、ペン、AC アダプタ	

（その他要件）

・全て未使用品とし、リサイクル品を認めない。

・システム全体が支障なく使用できる機器構成とすること。

・学校教育課で仕様を満たさない機器等が認められた場合は、速やかに入替えを行うものとする。

・特に端末スペックについては重視しており、発注者が選定を行う上で有益と思われるものについては審査の加点対象とする。

5.1.3. 既存環境との接続

・プリンタ

別添②「プリンタ等一覧」を参照

・無線 LAN

既存の学習系ネットワークに接続する。SSID 等情報は受託者へ提供することとする。

5GHz デジタル証明書なし、ID/パスワード認証 MAC フィルタなし

構築作業要件

本事業では、「GIGA スクール構想」を実現するための筑紫野市立小中学校 ICT 環境整備業務(以下、GIGA スクール)」で構築した、校内ネットワーク、無線アクセスポイントを校務環境でも利用することで、安全安心に配慮した、校務用サービス環境の実現を目指す。

6.1.1. 搬入等

・既存の校務用端末との入替スケジュールおよび計画書を作成し、教育委員会の承認を得ること。

・今回導入ハードウェア及びソフトウェア等の全てを一括して学校に搬入すること（宅配便等の利用は不可とする)。

・梱包材、廃材等はすみやかにすべて引き取ること。

・機器の搬入、調整及びこれらに付帯する工事に関わる費用はすべて含めること。

・搬入・設置に際して、校舎等施設を破損することがないこと。万一、搬入・設置時、または作業を行う際に、納入業者の責により校舎等施設を破損した場合は直ちに学校教育課へ破損の状況、原因等を報告し、納入業者が全額負担において修繕すること。

6.1.2. 構築業務要件

基本要件

(1) 5 年間運用できるシステムおよびハードウェアを選定すること。
(2) 調達する全てのソフトウェアは、原則、導入時の最新バージョンを導入すること。
(3) システムの運用に関して、本市で必要となる運用設計支援を行うこと。
(4) 教職員用端末はマルウェア対策、情報漏えいなどのセキュリティ対策をすること。ログの取得を前提とし、インシデント発生時など市の要望に応じてレポートを提出すること。

プロジェクト体制

(1) プロジェクト体制表の作成にあたっては、作業責任者、役割、連絡先を明確にすること。
(2) プロジェクトマネージャーまたは作業責任者について、以下の各条件を満たすこと。
(ア) システム設計・構築・運用等の業務経験を 5 年以上有していること。
(イ) 福岡県内や近郊のサポート経験を有すること。
(ウ) MS 365 に関する構築・運用保守業務の実績を保有すること。
(エ)「プロジェクトマネージャー」等の IPA が認定する高度認定資格、又は同等の資格を保有していること。

プロジェクト管理

(1) 本システムの導入過程の経過、進捗状況を、定例会議（月１回）を通じて報告すること。また進捗報告書及び打合せ会議に際しては、議事内容を事前に提示するとともに、毎回、受注者が議事録を作成し、会議終了後、速やかに提出すること。
(2) 本サービスの提供を進めていくうえで必要となる関係部署、関係機関との調整用資料等の作成についても支援すること。なお、課題や資料を随時共有できること。
(3) 設計、構築期間においては、必要に応じて検討会を実施し、スムーズな業務進行を図ること。また、仕様や要件の確認及び確定に関しては、必ず書面により行うこと。
(4) 課題管理表については、毎回の会議の中で確認を行うこと。

6.1.3. 設定・キッティング

・新規の校務用端末のマスターデータを作成し、展開すること。また、円滑な保守・運用のため、リカバリー媒体を作成すること。

・全ての新規の校務用端末でゼロトラスト型システム基盤を経由し、インターネット利用ができるように、設定作業と動作確認をおこなうこと。

・OS については、Windows 11 Pro 以上であること。

・管理に必要な番号等を機器に管理シール等で貼付しておくこと。(貼付方法や場所当は事前に教育委員会と協議すること。)

・校務用端末から Windows Defender の自動アップデートができるように設定すること。

・校務用端末入替に関わる利用者向け手順書を作成し、各教職員へ配布すること。

・引き渡し時には校務用端末の初期ログイン・パスワード変更の案内表を作成し、学校の業務に支障がないよう交換作業を行うこと。

・各校務用端末は認証基盤によるドメイン管理下に置くこと。

・校務ソフトウェア仕様以外のフリーソフトウェアについては学校教育課及び各学校と協議の上、各校務用パソコンにインストールすること。

・校務用端末に関する Windows アップデートに関しては、今回導入するシステムにより定期的にアップデートを行うよう設定を行うこと。

・その他校務用端末の環境設定に関する項目は別途学校教育課と協議の上､決定すること。

運用・保守性

7.1.1. システムメンテナンス

・利用者に影響のあるシステムへのメンテナンスは、可能な限り業務影響がない時間帯で実施すること。

・利用者に影響のあるメンテナンスを行う際には、事前に教育委員会と調整の上、エンドユーザーへの周知を行った上で実施すること。

7.1.2. 障害監視

・障害監視により異常を検知した場合は、メール等へ通知すること。

・Microsoft 管理センター等のポータルでサービスの正常性を目視確認できること。

テスト要件

8.1. 対象とするテストの範囲

8.1.1. システムテスト

・各サービス、サーバの正常系・異常系のテストを実施すること。
・バックアップおよびリストアテストについては、本市と必要性を協議の上で実施すること。

8.1.2. セキュリティテスト

・セキュリティ要件に記載の、アクセス制御・データ分類・情報漏洩対策については設計通りに動作することをシステムテストにて確認すること。
・ウイルス対策のテストについては、メーカーまたは一般に公開されているテストファイル等で実施すること。
・クラウドサービスやサーバへの侵入検知のテストまでは必須要件としないが、必要な場合はテスト計画に盛り込み協議の上適切な手続きを行った上で実施すること。

8.2. テストの実施方法

8.2.1. テスト実施計画

・テストは、本番運用を行う環境を用いて行うこと。

8.2.2. テスト環境

・本調達ではテスト環境の調達は想定していない。運用環境とは別にテスト環境を用意する場合は事業者負担で構築すること。

運用・保守要件

9.1. 運用・保守対象

・運用・保守対象とするシステムは以下とする。
- 本調達で構築するゼロトラスト型システム基盤全般
- 本調達で整備する校務用端末

9.2. 運用・保守内容

9.2.1. 運用内容

・　対象システムへの運用内容は以下とする。

No.	運用項目	運用内容
1	障害監視	システムの障害発生状況を監視し通知を行うこと。
2	一般的な問い合わせ対応	教職員等のエンドユーザーからの問合せに基づき操作方法の案内を行うこと。また不具合があった場合の一次問い合わせを受けつけること。
3	技術的な問い合わせ対応	システム管理者からの問合せに基づき運用業務および障害対応を行うこと。
5	システムメンテナンス	市教委と対応を協議の上、システムメンテナンスを行うこと。またクライアントの更新プログラム配信設定のメンテナンスも含む（例：Windows のバージョン固定の解除、次期バージョンの配信許可設定）
6	定例会	障害情報、セキュリティの情報、問合せの対応履歴について情報整理し市教委へ報告すること。（月 1 回程度想定）
7	ハードウェア保守	校務用端末の保守管理を行い、不具合が生じた場合は現地修理またはセンドバック等により速やかに対応可能な体制を準備すること。 校務用端末が不良になった場合、本市の責による場合を除き、出張修理を行うこと。（部品代を含む） ハードウェア修理のみではなく導入時の設定状態までの再設定を行うこと。 但し、以下のケースは保守対象外とする。 データの破損、紛失、機器の物理破損、本調達品以外を起因とした障害

9.2.2. 保守内容

・　対象システムへの保守内容は以下とする。

No.	保守項目	保守内容
1	障害対応・復旧作業	利用者からの問い合わせ、ならびに障害監視結果を基に、障害対応・復旧作業を遠隔・現地で行うこと。
2	保守履歴管理	障害対応・復旧作業で実施した保守内容の管理を行うこと。

9.2.3. 運用保守体制

・運用保守の問合せ窓口を開設すること。

・問合せ窓口は以下の要件を満たすこと。

- 平日（土・日・祝祭日・年末年始以外）9:00-17:00 メールおよび電話での問合せ対応
- 時間外のメールによる問合せに対しては、翌営業日に対応すること

・ただし、授業影響が発生するような緊急を要する障害が発生した際には、市教育委員会と協議の上、速やかに対応すること。

9.3. 運用・保守提供時間

・開庁日（日曜日、土曜日、国民の祝日に関する法律「昭和 23 年法律第 178 号」に規定する休日及び 12 月 29 日から翌年 1 月 3 日までの日は除く。）の 9 時 00 分から 17 時 30 分までの間とする。ただし、システム利用に致命的な障害が発生した際は、協議の上、速やかに対応を行うこと。
・開庁日内で対応が不可能な日程が存在する場合は、事前に市教育委員会に報告し承認を得ること。

9.4. その他保守事項

システムが末永く安定稼動するよう体制を整え、メンテナンスを行うこと。

① 障害復旧時には、障害の事象、影響、原因及び対策方法等をまとめた報告書を作成し、提出すること。
② ハードウェア・ソフトウェア・サービスともに、製品及び技術に関する情報提供を行うこと。
③ 各システムの日々の運用における次の軽微な作業については、筑紫野市にて実施する。
・年度末以外のタイミングでの配属・異動・退職等におけるユーザーアカウントの管理
・ファイル管理機能内でのファイル復元作業
・各種サーバの状態確認
・定期的なイベントログ確認等
④ 同ネットワーク内の他システムとの調整が必要なものに関しても最大限協力するものとする。
⑤ サービスパック・パッチ等については速やかに情報を入手し適用すること。
⑥ セキュリティパッチについては、スケジュールを組んで定期的に適用する仕組みとすること。
⑦ 無償あるいは保守の範囲でバージョンアップの権利を有するものについては時期を見極め積極的に適用すること。
⑧ 基本的に営業時間内でのコールを原則に経費を見積ること。
⑨ リモート保守を行う際は、 筑紫野市への接続が許可された特定端末により、セキュリティが確保されたエリアからのみ行うこととする。また、接続の際は筑紫野市の許可を得るようにする。

説明会・研修の計画

10.1. 説明会・研修

・研修対象者に即したマニュアルの作成も業務範囲とする。

・研修についてはオンラインおよび対面のいずれの形式も可とする。
・オンラインで開催する際には、当日やむを得ず欠席となった利用者を配慮し、録画したデータをストリーミング形式で受講可能とする。また、録画データは一般的な端末で視聴可能なデータ形式で提供すること。
・研修会実施後に発生する研修対象者からの問い合わせを受け付ける窓口を設けること。
・オンライン研修の内容
  - 管理者向け（教育委員会）
  - 管理職・情報担当者向け
  - 教職員向け
  - ICT 支援員向け
・オンライン研修の形式
  - 集合研修
  - オンライン

想定している研修対象者、研修内容、研修方法、開催時期/回数は以下とするが、詳細な内容や開催日程については、教育委員会と別途協議の上で決定すること。

受講者分類	研修対象者	研修内容	方法	開催時期/回数
シ ス テ ム 管理者	教育委員会システム担当	年次更新業務についての説明 管理ポータルの使用方法	集合研修	導入後 1 回以上
管理職・情報担当	学校管理職・各学校の情報担当	システムの利用方法および管理職向け・情報担当向けの機能説明	集合研修またはオンライン	導入後 1 回以上
一般教職員	学校の教職員（管理職・情報担当を除く）	システムの利用方法 問合せ方法の説明	集合研修またはオンライン	導入後 1 回以上
ICT 支援員	市内に配備された ICT 支援員	システムの利用方法 問合せ方法の説明	集合研修またはオンライン	導入後 1 回以上

成果品等

11.1. 完了時提出書類

本業務が完了した際は、受注者は本市指定の完了届を本市に提出するものとする。

11.2. 成果品検査等

業務の完了後、成果品を提出し本市の検査を受けるものとし、本業務に適しないものとして修正の指示があった場合には、速やかに修正を行うものとする。

また、本業務の完了後であっても、成果品に瑕疵が発見された場合には、本市の指示に従い速やかに成果品の修正を行なわなければならない。この場合において、当該修正に要する費用は、全て受注者の負担とする。

11.3. 成果品

・以下に掲げる成果品を製本及び電子媒体で納品すること

ア．システム基本設計書（製本・PDF 各１部）

イ．システム詳細設計書（製本・PDF 各１部）

ウ．システム移行スケジュール（製本・PDF 各１部）

エ．校務用端末 設定・パラメータ資料（製本・PDF 各１部）

オ．校務用端末 キッティングチェックシート（製本・PDF 各１部）

カ．校務用端末 学校毎のシリアル・管理番号一覧表（製本・PDF 各１部）

キ．校務用端末 納入写真（製本・PDF 各１部）

ク．システム ID・パスワード一覧（製本・PDF 各１部）

ケ．システム試験成績表（製本・PDF 各１部）

コ．管理者向け運用マニュアル・障害対応マニュアル（製本・PDF 各１部）

サ．教職員向け基本操作マニュアル（製本・PDF 各１部）

わかりやすい内容で双方の担当者に異動が生じても速やかに引き継ぎができるようにすること

シ．その他必要と思われるドキュメントがあれば同様に納品すること

※ 電子ファイルは１枚のメデイアに集約すること

※「試験成績表」以外については後の改修・運用変更に備え、できるだけ編集可能なファイル形式でも納品し、加除整理を行うこと。

・電子媒体による報告書は、CD-R または DVD-R に業務名を印刷して 1 部提出すること。

・校務用端末の不要な取扱説明書や付属品は教育委員会及び各学校に各一部保管とする。

・本業務は、補助金等を活用した業務になることから、実績報告書等に必要となる資料（内容については契約後指示）についても提出すること。

・契約満了後においても、報告書等の内容について、本市からの問い合わせや根拠資料の提出要求があった際には、適宜対応すること。

11.4. 成果品の納入場所

〒818－8686 福岡県筑紫野市石崎 1-1-1 筑紫野市教育委員会学校教育課

11.5. 成果品の管理及び帰属

本業務の成果品は全て本市の管理及び帰属とし、受注者は成果品を第三者に公表又は貸与してはならない。

11.6. その他

・本業務は、本仕様書に基づき実施すること。
・受注者は業務の進歩状況等を定期的に報告するほか、本市の求めに応じて速やかに報告を行うものとする。
・本業務の実施にあたっては、関係法令、条例及び規則を遵守すること。
・本業務の遂行上知り得た秘密を他人に漏らしてはならない。
・本仕様書に定めのない事項や業務の実施にあたり疑義が生じた場合は、速やかに本市と協議のうえ定めるものとする。