《二者契約用》

賃　貸　借　契　約　書　（案）

兵庫県立神崎高等学校（以下「甲」という。）と＿＿＿＿＿＿（以下「乙」という。）とは、（賃貸借物品）　（以下「物件」という。）の賃貸借及びソフトウェアの提供について、次の条項に従うほか、関係法令を遵守し、信義誠実の原則を守り、これを履行するものとする。

（対象物件及び設置場所）
第１条　甲は、乙から別表の物件を賃借し、乙は、甲に当該物件を賃貸する。
２　物件、提供を受けるソフトウェア及び設置場所は、仕様書記載のとおりとする。
３　この契約でソフトウェアとは、甲が、著作権者等適法な権原を有する者との間でソフトウェアの使用許諾契約を締結することを前提に、乙から提供されるものをいい、記憶媒体、パッケージ及び取扱説明書等を含む。
（契約期間）
第２条　契約期間は、令和７年３月 31 日から令和 12 年３月 30 日までとする。
（賃貸借料）
第３条　賃貸借料（ソフトウェアの提供料を含む。以下同じ。）は、月額金＿＿＿＿＿＿円（うち消費税及び地方消費税の額金＿＿＿＿＿＿円）とする。ただし、令和７年３月 31 日に限っては日額金＿＿＿＿＿＿円（うち消費税及び地方消費税の額金＿＿＿＿＿＿円）とする。
２　契約期間中に１か月未満の端数を生じた月、又は乙の責に帰すべき理由により物件を使用できなかった月の賃貸借料は、日割計算（次式）により算出するものとする。なお、当該金額に１円未満の端数を生じるときは、その金額を切り捨てるものとする。（月額賃貸借料金／当月の暦日数×当月賃貸借日数）
（賃貸借料の請求）
第４条　乙は、毎月 10 日までに前月分の賃貸借料を甲に請求するものとする。
（賃貸借料の支払）
第５条　甲は、前条の規定により乙から正当な請求書を受理した日から 30 日以内に賃貸借料を乙に支払うものとする。ただし、特別の理由がある場合は、この限りでない。
（契約保証金）
第６条　①契約保証金は、金＿＿＿＿＿＿円とする。
②財務規則（昭和 39 年兵庫県規則第 31 号）第 100 条第１項第１号の規定により、契約保証金を免除する。
③財務規則（昭和 39 年兵庫県規則第 31 号）第 100 条第１項第３号の規定により、契約保証金を免除する。
《※場合により①～③のいずれかを記載すること》
（秘密の保持）
第７条　乙は、この契約の履行に関して直接又は間接に知り得た秘密を他人に漏らし、又は他の目的に使用してはならない。なお、この契約が終了し、又は解除された後においても同様とする。
２　乙は、甲から提供された資料、原票等（以下「資料等」という。）については、甲の承諾なくして複写又は複製をしてはならない。また、この契約の履行中においては、資料等を善良なる管理者の注意をもって保管するとともに、使用後は速やかに甲に返還するものとする。
（個人情報の保護）
第８条　乙は、この契約を履行するための個人情報の取扱いについては、別記「個人情報

取扱特記事項」を守らなければならない。

（セキュリティ対策）

第９条　乙は、この契約の履行における情報セキュリティ対策のために、「兵庫県情報セキュリティ対策指針」及び「兵庫県教育情報セキュリティ対策基準」を守らなければならない。

２　甲は、乙が前項の規定に違反し甲に損害を与えたときは、乙に対して損害の賠償を請求することができる。

３　甲は、セキュリティ対策の実施状況確認のため、随時に、調査し、若しくは必要な報告を求め、又はセキュリティ対策に関して乙に改善を求めることができる。

（権利、義務の譲渡禁止）

第 10 条　乙は、この契約により生ずる権利又は義務を第三者に譲渡し、又は承継させてはならない。ただし、甲の書面による承認を受けた場合は、この限りでない。

（委託の禁止）

第 11 条　乙は、この契約の全部又は主体的部分を一括して第三者に委任し、又は請け負わせてはならない。

２　前項における主体的部分とは、この契約における総合的な企画及び判断並びに管理部分をいう。

３　乙は、この契約の一部を第三者に委任し、又は請け負わせ（以下「一部委託」という。）てはならない。ただし、あらかじめ一部委託の相手方の住所、氏名及び一部委託を行う業務の範囲等（以下「一部委託に関する事項」という。）を記載した一部委託の必要性がわかる書面を甲に提出し、甲の書面による承認を得た場合は、乙は、甲が承認した範囲の業務を第三者（以下「承認を得た第三者」という。）に一部委託することができる。

４　前項ただし書きにより甲が承認した場合には、承認を得た第三者も、前項の義務を負うものとし、乙は、当該第三者に前項の義務を遵守させるために必要な措置をとらなければならない。その後に承認を得た第三者についても、同様とする。

５　乙は、この契約の一部を一部委託先から、さらに第三者に再委託させる場合（２次委託）には、甲に対し、当該第三者の一部委託に関する事項を記載した書面を提出し、甲の書面による承認を受けなければならない。なお、３次委託以降も同様とする。

６　一部委託する相手方の変更等を行おうとする場合には、乙は、改めて一部委託に関する事項が記載された書面を提出し、甲の承認を受けなければならない。

７　乙は、この契約の一部を一部委託する場合には、一部委託した業務に伴う承認を得た第三者の行為について、甲に対し全ての責任を負うものとする。

（使用及び管理）

第 12 条　甲は、善良な管理者の注意をもってソフトウェアを使用及び管理するものとする。

２　物件に故障が生じたときは、甲は直ちに乙に報告するものとする。

（物件の維持及び費用）

第 13 条　乙は、故障を発見したとき、又は前条第２項の規定により甲から故障の通知があったときは、遅滞なく乙の責任において、物件が良好な状態で稼動できるよう必要な費用を負担して修理（天災その他の不可抗力による故障の修理を含む。）するものとし、設置場所での修理が困難な場合は、修理期間中無償で代替機と交換するものとする。ただし、甲の責に帰すべき理由によってその修理又は交換が必要になったときは、この限りでない。

２　甲は、物件の修理が必要である場合において、次に掲げるときは、その修理をすることができるものとする。

（１）乙が、前項に規定する通知があってから相当の期間内に必要な修理をしないとき。

（２）急迫の事情があるとき。
３　前項の場合において、甲は、その修理に要した費用を支出したときは、乙に対してその費用の償還を請求できるものとする。ただし、甲の責に帰すべき理由によってその修理が必要になったときは、この限りでない。
４　乙は、物件が正常に動作するよう、乙の費用負担において、必要な保守を行う。ただし、通常の保守を超える特別な保守を必要とする場合の費用は、甲の負担とする。
５　乙は当該物件を契約日までに納入しなければならない。ただし、特別な事情により期日までに納入が困難な場合は、納入できるまでの間同等の機能を有する代替機を用意しなければならない。

（消耗品の使用制限）
第 14 条　甲は物件に使用する消耗品について、乙の定める規格に合致したものを使用するものとする。
２　前項に定める規格以外のものを使用して生じた物件の事故については、甲の責任とする。

（ソフトウェアの使用）
第 15 条　甲は、ソフトウェアを物件以外の装置に使用し、又は複製してはならない。ただし、第１条第３項のソフトウェア使用許諾契約に認められている範囲で乙の承諾を得た場合は、この限りではない。
２　甲は、ソフトウェアを第三者に提供してはならない。
３　乙は、甲の円滑な業務遂行に協力するため、ソフトウェア及びオペレーションについて、甲の職員に講習会等の技術サービスを、乙の定めた基本サービスの範囲内で無償で行うものとする。

（技術支援等）
第 16 条　乙は必要に応じてソフトウェアのインストール、トラブル処理等に関する技術支援を行うものとする。

（所有者の表示）
第 17 条　乙は、物件に自己の所有である旨の表示を付することができる。

（保険）
第 18 条　乙は、物件につき乙の費用で動産総合保険を付保するものとする。

（履行遅滞の場合の違約金）
第 19 条　乙は、その責に帰すべき理由により、契約の履行期限内に契約を履行しないときは、契約の履行期限の翌日から履行の日までの日数に応じ、契約金額（月額賃貸借料金×契約月数）につき年 10.75％の割合で計算した額を違約金として甲に納めなければならない。

（損害賠償）
第 20 条　乙は、甲が故意又は重大な過失によって物件に損害を与えたときは、その賠償を甲に対して請求できるものとする。ただし、甲が物件を修理し、又は乙が動産総合保険で補償された場合は、その範囲内において甲は賠償の責を負わないものとする。

（搬入・搬出料金）
第 21 条　物件の搬入及び搬出に要する費用は、乙の負担とする。

（甲の通知義務）
第 22 条　甲は、物件について改造又は仕様の変更をしようとするときは、乙に事前に書面で通知し、その承諾を得るものとする。
２　甲は、物件及びソフトウェアについて盗難、滅失、損傷等の事故が発生したときは、遅滞なく乙に通知するものとする。

（物件の返還）

第 23 条　甲は、契約期間が満了したとき又は契約を解除したときは、設置場所において物件を乙に返還するものとする。
２　前項の場合において、甲は、物件を受け取った後にこれに生じた損傷（通常の使用及び収益によって生じた物件の損耗並びに物件の経年劣化を除く。）があるときは、その損傷を原状に復さなければならない。ただし、その損傷が甲の責に帰することができない理由によるものであるときは、この限りでない。
（契約の解除）
第 24 条　甲は、乙が、次の各号のいずれかに該当する場合においては、相当の期間を定めてその履行の催告をし、その期間内に履行がないときは、この契約を解除することができる。ただし、その期間を経過した時における債務の不履行がこの契約及び取引上の社会通念に照らして軽微であるときは、この限りでない。
（１）契約の履行期限内に契約を履行しないとき、又は契約を履行する見込みがないと明らかに認められるとき。
（２）乙又はその代理人その他の使用人が検査を妨げたとき。
第 24 条の２　甲は、乙が次の各号のいずれかに該当する場合においては、直ちにこの契約を解除することができる。
（１）法令の規定により、営業に関する許可を取り消され、又は営業の停止を命じられたとき。
（２）乙又はその代理人が、関係法令又は契約事項に違反し、そのため契約の目的を達することができない、又は契約を継続することが適当でないと認められるとき。
（３）乙又はその代理人、支配人その他の使用人若しくは入札代理人として使用していた者が、この契約の入札に関して地方自治法施行令（昭和 22 年政令第 16 号）第 167 条の４第２項第２号に該当すると認めたとき。
第 24 条の３　甲は、第 24 条各号又は前条各号に規定する場合が甲の責に帰すべき理由によるものであるときは、前２条の規定による契約の解除をすることができない。
２　甲は、翌年度以降の歳入歳出予算において、この契約にかかる予算の減額又は削除があったときは、この契約を解除することができる。
３　甲は、前２条及び前項に規定する場合のほか、特に必要があるときは、この契約を解除することができる。
４　前２条の規定による解除に伴い、乙に損害が生じたとしても、乙は、甲に対してその損害の賠償を請求することはできない。
５　第２項又は第３項の規定により契約が解除された場合に、乙に損害が生じたときは、乙は、甲に対してその損害の賠償を請求することができる。
６　前２条の規定により、この契約を解除した場合においては、乙は、次の各号による金額を違約金として甲の指定する期限までに甲に納付しなければならない。ただし、この契約を解除した場合が、この契約及び取引上の社会通念に照らして乙の責に帰することができない理由によるものであるときは、この限りでない。
（１）賃貸借開始日前に解除した場合には、契約金額の 10 分の１に相当する額。
（２）賃貸借開始日以降に解除した場合には、当該解除日の翌日から本契約期間の満了日までの期間に対する契約金額の 10 分の１に相当する額。
７　前項の場合において、契約保証金の納付またはこれに代わる担保の提供が行われているときは、甲は、当該契約保証金又は担保をもって違約金に充当することができる。
８　甲は、この契約を解除しようとするときは、その理由を記載した書面により、乙に通知するものとする。
（暴力団等の排除）
第 25 条　甲は、次条第１号の意見を聴いた結果、乙が次の各号のいずれかに該当する者

（以下「暴力団等」という。）であると判明したときは、特別の事情のある場合を除き、契約を解除するものとする。

（１）暴力団排除条例(平成 22 年兵庫県条例第 35 号)第２条第１号に規定する暴力団及び第３号に規定する暴力団員

（２）暴力団排除条例施行規則（平成 23 年兵庫県公安委員会規則第２号）第２条各号に規定する暴力団及び暴力団員と密接な関係を有する者

２　前条第４項及び第６項から第８項までの規定は、前項の規定による契約の解除に準用する。

（情報の利用）

第 26 条　甲は、必要に応じ、次の各号に掲げる措置を講じることができるものとする。

（１）乙が暴力団等であるか否かについて兵庫県警察本部長に意見を聴くこと。

（２）前号の意見の聴取により得た情報を、他の契約において暴力団等を排除するための措置を講じるために利用し、又は兵庫県、兵庫県公営企業管理者及び兵庫県病院事業管理者に提供すること。

（警察の捜査への協力）

第 27 条　乙は、この契約の履行に当たり、暴力団等から業務の妨害その他不当な要求を受けたときは、甲にその旨を報告するとともに、警察に届け出て、その捜査等に協力しなければならない。

（適正な労働条件の確保）

第28条　乙は、この契約における労働者の適正な労働条件を確保するため、別記「適正な労働条件の確保に関する特記事項」を守らなければならない。

（賠償の予約）

第29条　乙は、乙又はその代理人、支配人その他使用人若しくは入札代理人として使用していた者が、この契約の入札に関して次の各号のいずれかに該当したときは、契約金額の10分の２に相当する額を賠償金として甲が指定する期限までに甲に支払わなければならない。物品の納入後も同様とする。

（１）刑法（明治40年法律第45号）第96条の６による刑が確定したとき。

（２）刑法第198条による刑が確定したとき。

（３）公正取引委員会が、私的独占の禁止及び公正取引の確保に関する法律（昭和22年法律第54号。以下「独占禁止法」という。）第61条第１項の規定による排除措置命令を行ったとき。ただし、排除措置命令に対し、行政事件訴訟法（昭和37年法律第139号）第３条第１項の規定により抗告訴訟を提起した場合を除く。

（４）公正取引委員会が、独占禁止法第62条第１項の規定による課徴金納付命令を行ったとき。ただし、課徴金納付命令に対し、行政事件訴訟法（昭和37年法律第139号）第３条第１項の規定により抗告訴訟を提起した場合を除く。

（５）前２号の抗告訴訟を提起し、その訴訟について請求棄却又は訴え却下の判決が確定したとき。

２　前項の規定は、甲に生じた損害の額が同項に規定する賠償金の額を超える場合において、甲がその超過分につき賠償を請求することを妨げるものではない。

（調査への協力）

第 30 条　甲は、この契約に係る甲の適正な予算執行を検証するため、必要があると認めた場合は、乙に対し、甲が行う調査に必要な物品の出納に関する帳簿の閲覧又は情報の提供等の協力を要請することができる。

２　乙は、甲から前項の要請があった場合は、特別な理由がない限りその要請に応じるものとし、この契約の終了後も、契約終了日の属する県の会計年度を含む６会計年度の間は同様とする。

（その他）
第 31 条　この契約に定めのない事項、又はこの契約に疑義のある場合は、財務規則（昭和 39 年兵庫県規則第 31 号）によるほか、甲、乙協議の上、定めるものとする。

この契約の証として本書２通を作成し、甲、乙記名押印の上、各自その１通を保有する。

令和　　年　　月　　日

甲　住　　所
商号又は名称
代表者氏名

乙　住　　所
商号又は名称
代表者氏名

《二者契約用》

誓　約　書

暴力団排除条例（平成22年兵庫県条例第35号。以下「条例」という。）を遵守し、暴力団排除に協力するため、下記のとおり誓約する。

記

1　条例第２条第１号に規定する暴力団、又は第３号に規定する暴力団員に該当しないこと
2　暴力団排除条例施行規則（平成23年兵庫県公安委員会規則第２号）第２条各号に規定する暴力団及び暴力団員と密接な関係を有する者に該当しないこと
3　上記１及び２に違反したときには、本契約の解除、違約金の請求その他県が行う一切の措置について異議を述べないこと

令和　　年　　月　　日

兵庫県立　　高等学校長　様

住　　所
会 社 名
代表者名
電　　話
電子メール

（別紙）

【個人情報取扱特記事項】

（基本的事項）

第１　乙は、個人情報の保護の重要性を認識し、この契約による事務を実施するに当たっては、関係法令等の規定に従い、個人の権利利益を侵害することのないよう、個人情報の取扱いを適切に行わなければならない。

（収集の制限）

第２　乙は、この契約による事務を行うために個人情報を収集するときは、事務の目的を達成するために必要な範囲内で、適法かつ公正な手段により行わなければならない。

（目的外利用・提供の制限）

第３　乙は、甲の指示がある場合を除き、この契約による事務に関して知ることのできた個人情報を契約の目的以外の目的に利用し、又は甲の承諾なしに第三者に提供してはならない。

（安全管理措置）

第４　乙は、この契約による事務に関して知ることのできた個人情報について、個人情報の漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

（廃棄）

第５　乙は、この契約による事務に関して知ることのできた個人情報について、保有する必要がなくなったときは、確実かつ速やかに廃棄し又は消去し、甲に報告しなければならない。

（秘密の保持）

第６　乙は、この契約による事務に関して知ることのできた個人情報をみだりに他人に知らせてはならない。この契約が終了し、又は解除された後においても、同様とする。

（複写又は複製の禁止）

第７　乙は、この契約による事務を処理するために甲から引き渡された個人情報が記録された資料等を甲の承諾なしに複写又は複製してはならない。

（特定の場所以外での取扱いの禁止）

第８　乙は、この契約による事務を処理するために個人情報を取り扱うときは、甲の事務室内において行うものとし、甲が承諾した場合を除き、当該場所以外の場所で個人情報を取り扱ってはならない。

（事務従事者への周知及び指導・監督）

第９　乙は、その事務に従事している者に対して、在職中及び退職後においてもこの契約による事務に関して知ることのできた個人情報をみだりに他人に知らせ、又は不当な目的に使用してはならないことなど、個人情報の保護に必要な事項を周知し、適切な取扱いがなされるよう指導・監督するものとする。

（責任体制の整備）

第10　乙は、この契約による個人情報の取扱いの責任者及び事務従事者の管理体制・実施体制を定め、甲に書面で報告しなければならない。

２　乙は、前項の責任者及び事務従事者を変更する場合は、甲に報告しなければならない。

（一部委託の禁止）

第11　乙はこの契約の一部を第三者（乙の子会社を含む。）に委任し、又は請け負わせ（以下「一部委託」という。）てはならない。ただし、あらかじめ一部委託の相手方の住所、氏名及び一部委託を行う業務の範囲等（以下「一部委託に関する事項」という。）を記載した一部委託の必要性がわかる書面を甲に提出し、甲の書面による承認を得た場合は、乙は、甲が承認した範囲の業務を第三者（以下「承認を得た第三者」という。）に一部委託することができる。

２　前項ただし書きにより甲が承認した場合には、承認を得た第三者も前項の義務を負うものとし、乙は、当該第三者に前項の義務を遵守させるために必要な措置をとらなければならない。その後に承認を得た第三者についても同様とする。

３　乙は、この契約の一部を一部委託先から、さらに第三者に再委託させる場合（２次委託）には、甲に対し、当該第三者の一部委託に関する事項を記載した書面を提出し、甲の書面による承認を受けなければならない。なお、３次委託以降も同様とする。

４　一部委託する相手方の変更等を行おうとする場合には、乙は、改めて一部委託に関する事項が記載された書面を提出し、甲の承認を受けなければならない。

５　乙は、この契約の一部を一部委託する場合には、一部委託した業務に伴う承認を得た第三者の行為について、甲に対し全ての責任を負うものとする。

６　乙は、一部委託先に対して、その委託した業務の履行状況を管理・監督するとともに、甲の求

めに応じて、管理・監督の状況を甲に対して適宜報告しなければならない。

（資料等の返還等）

第12　乙は、この契約による事務を処理するために、甲から提供を受け、又は乙自らが収集し、若しくは作成した個人情報が記録された資料等は、この契約完了後直ちに甲に返還し、又は引き渡すものとする。ただし、甲が別に指示したときは当該方法によるものとする。

（立入調査）

第13　甲は、乙及び一部委託先が契約による事務の執行に当たり取り扱っている個人情報の状況について、随時調査することができる。

（遵守状況の報告）

第14　甲は、必要があると認めるときは、この契約が求める個人情報の取扱いに係る遵守状況の報告を乙に求めること及び当該取扱いについて乙に適切な措置をとるよう指示することができる。

２　乙は、前項の報告の求め又は指示があった場合は、速やかに応じなければならない。

（事故発生時における報告）

第15　乙は、この契約に関し個人情報の漏えい等の事故が発生した場合は、その事故の発生に係る帰責の有無に関わらず、直ちに甲に対して、当該事故に関わる個人情報の内容、件数、事故の発生場所、発生状況を書面により報告し、甲の指示に従わなければならない。

２　乙は、個人情報の漏えい等の事故が発生した場合に備え、甲その他の関係者との連絡、証拠保全、被害拡大の防止、復旧、再発防止の措置を迅速かつ適切に実施するために、緊急時対応計画を定めなければならない。

３　甲は、この契約に関し個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。

（契約の解除）

第16　甲は、乙が本特記事項に定める義務を果たさない場合は、この契約による業務の全部又は一部を解除することができるものとする。

２　乙は、前項の規定に基づく契約の解除により損害を被った場合においても、甲にその損害の賠償を求めることはできない。

（損害賠償）

第17　甲は、乙が本特記事項に定める規定に違反し、又は怠ったことにより損害を被った場合には、乙に対して損害の賠償を求めることができる。

《二者契約用》

【適正な労働条件の確保に関する特記事項】

（基本的事項）

第１　乙は、別表に掲げる労働関係法令（以下「労働関係法令」という。）を遵守することにより、次の各号のいずれかに該当する労働者（以下「特定労働者」という。）に対する最低賃金法（昭和34年法律第137号）第３条に規定する最低賃金額（同法第７条の規定の適用を受ける労働者については、当該最低賃金額から同条の規定により減額した額。以下「最低賃金額」という。）以上の賃金の支払その他の特定労働者の適正な労働条件を確保しなければならない。

（１）乙に雇用され、この契約に基づく業務に関わっている労働基準法（昭和22年法律第49号）第９条に規定する労働者（当該業務に直接従事しない者や家事使用人を除く。）

（２）労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和60年法律第88号。以下「労働者派遣法」という。）の規定により、乙のためにこの契約に基づく業務に関わっている労働者（以下「派遣労働者」という。当該業務に直接従事しない者を除く。）

２　乙は、当該者を発注者とする下請契約を締結する場合においては、この特記事項の第１から第５までの規定に準じた規定を当該下請契約に定めなければならない。

（受注関係者に対する措置）

第２　乙がこの契約に基づく業務の一部を第三者に行わせようとする場合の当該受託者及び当該契約に基づく業務に派遣労働者を関わらせようとする場合の当該派遣契約の相手方（以下「受注関係者」という。）は、労働関係法令を遵守することを誓約した者でなければならない。

２　乙は、前項の場合において、その契約金額（同一の者と複数の契約を締結した場合には、その合計金額。）が200万円を超えるときは、当該受注関係者から労働関係法令を遵守する旨等を記載した誓約書を徴取し、その写し（第１の第２項の規定により、この項に準じて下請契約等に定めた規定により提出させた誓約書の写しを含む。）を甲に提出しなければならない。

３　乙は、受注関係者又は下請その他いかなる名義によるかを問わず県以外の者から、この契約に係る業務の一部について請け負った者（以下「下請関係者」という。）が労働関係法令を遵守していないと認めるときは、当該受注関係者に対し、指導その他の特定労働者（下請関係者に雇用され、この契約に基づく業務に関わっている労働者を含む。以下同じ。）の適正な労働条件を確保するために必要な措置を講じなければならない。

４　乙は、受注関係者が次の各号のいずれかに該当するときは、当該受注関係者と締結している契約を解除しなければならない。

（１）乙に対し第４の第４項、第５の第３項若しくは第４項の規定による報告をせず、又は虚偽の報告をしたとき。

（２）特定労働者に対する賃金の支払について、最低賃金法第4条第1項の規定に違反したとして、検察官に送致されたとき。

（特定労働者からの申出があった場合の措置）

第３　甲は、特定労働者から、乙又は下請関係者が特定労働者に対して最低賃金額以上の賃金を支払っていない旨の申出があった場合においては、当該申出の内容を労働基準監督署に通報するものとする。

２　甲は、前項の場合においては、必要に応じ、乙に対し、労働基準監督署への通報に必要な情報について報告を求めることができる。

３　乙は、前項の報告を求められたときは、速やかに甲に報告しなければならない。

４　乙は、その雇用する特定労働者が第１項に規定する申出をしたことを理由として、当該特定労働者に対し、解雇その他の不利益な取扱いをしてはならない。

５　乙は、第１項に規定する特定労働者が下請関係者に雇用されている場合において、第２項の報告を求められたときは、受注関係者に対して確認を行い、当該確認の結果を甲に報告しなければならない。

６　乙は、下請関係者に雇用されている特定労働者が第１項に規定する申出をしたことを理由として、当該下請関係者が当該特定労働者に対し、解雇その他の不利益な取扱いをしないよう、受注関係者に求めなければならない。

７　甲は、必要に応じ、労働基準監督署に対し、第３項、第５項、第４の第２項、第４項及び第５の各項の規定による甲に対する報告により得た情報を提供することができる。

（労働基準監督署から意見を受けた場合の措置）

第４　甲は、労働基準監督署から乙に雇用されている特定労働者の賃金が最低賃金額に達しない旨の意見を受けたときは、乙に対し、当該特定労働者に最低賃金額以上の賃金の支払を行うことを求めるものとする。

２　乙は、前項の規定により賃金の支払を行うよう求められたときは、甲が定める期日までに当該支払の状況を甲に報告しなければならない。

３　甲は、労働基準監督署から下請関係者に雇用されている特定労働者の賃金が最低賃金額に達しない旨の意見を受けたときは、乙に対し、当該特定労働者に最低賃金額以上の賃金の支払を行う旨の指導を受注関

係者に行うことを求めるものとする。
4　乙は、前項の規定により指導を行うよう求められたときは、同項の受注関係者に対して同項の賃金の支払の状況の報告を求めるとともに、甲が定める期日までに当該報告の内容を甲に報告しなければならない。

（労働基準監督署から行政指導があった場合の措置）
第５　乙は、労働基準監督署長又は労働基準監督官から特定労働者に対する賃金の支払における最低賃金法の違反について行政指導を受けた場合においては、速やかに当該行政指導を受けたこと及びその対応方針を甲に報告しなければならない。
２　乙は、前項の場合において、同項の違反を是正するための措置（以下「是正措置」という。）を行い、その旨を労働基準監督署長又は労働基準監督官に報告したときは、速やかに是正措置の内容を甲に報告しなければならない。
３　乙は、下請関係者が第１項の行政指導を受けた場合においては、受注関係者に対して速やかに当該行政指導を受けたこと及びその対応方針について報告を求めるとともに、当該報告の内容を甲に報告しなければならない。
４　乙は、前項の場合において、同項の下請関係者が是正措置を行い、その旨を労働基準監督署長又は労働基準監督官に報告したときは、受注関係者に対して速やかに当該是正措置の報告を求めるとともに、当該報告の内容を甲に報告しなければならない。
（契約の解除）
第６　甲は、次の各号のいずれかに該当するときは、契約を解除することができる。
（１）乙が、甲に対し第４の第２項、第５の第１項若しくは第２項の規定による報告をせず、又は虚偽の報告をしたとき。
（２）乙が、甲に対し第４の第４項、第５の第３項若しくは第４項の規定による報告をせず、又は虚偽の報告をしたとき。（乙が、第２の第１項の誓約をした受注関係者に対して、第４の第３項に規定する指導及び第４の第４項、第５の第３項又は第４項の規定による報告の求めを行ったにもかかわらず、当該受注関係者が乙に対して当該報告をせず、又は虚偽の報告をしたときを除く。）
（３）特定労働者に対する賃金の支払について、乙又は受注関係者が最低賃金法第4条第1項の規定に違反したとして、検察官に送致されたとき。（乙が第２の第４項の規定により、当該受注関係者と締結している契約を解除したときを除く。）
（損害賠償）
第７　乙は、第６の規定による契約の解除に伴い、損害が生じたとしても、甲に対してその損害の賠償を請求することはできない。
（違約金）
第８　乙は、第６の規定により契約が解除された場合は、違約金を甲の指定する期限までに甲に支払わなければならない。

別表（第１関係）

労働関係法令
(1) 労働基準法（昭和22年法律第49号）
(2) 労働組合法（昭和24年法律第174号）
(3) 最低賃金法（昭和34年法律第137号）
(4) 労働安全衛生法（昭和47年法律第57号）
(5) 雇用の分野における男女の均等な機会及び待遇の確保等に関する法律（昭和47年法律第113号）
(6) 労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和60年法律第88号）
(7) 短時間労働者及び有期雇用労働者の雇用管理の改善等に関する法律（平成5年法律第76号）
(8) 労働契約法（平成19年法律第128号）
(9) 健康保険法（大正11年法律第70号）
(10) 厚生年金保険法（昭和29年法律第115号）
(11) 雇用保険法（昭和49年法律第116号）
(12) 労働保険の保険料の徴収等に関する法律（昭和44年法律第84号）

《二者契約用》

誓　約　書

下記１の契約（以下「本契約」という。）に基づく業務に従事する労働者の適正な労働条件を確保するため、下記２の事項を誓約する。

記

１　契約名

（賃貸借物品）賃貸借契約

２　誓約事項

（１）本契約に基づく業務に関わっている労働者に対し最低賃金額以上の賃金の支払を行うこと、及び別表に掲げる労働関係法令を遵守すること。

（２）本契約に基づく業務に関わっている労働者に対する賃金の支払について次に該当するときは、速やかに県へ報告を行うこと。

ア　県から最低賃金額以上の賃金の支払を行うよう指導を受けその報告を求められたとき。

イ　労働基準監督署から最低賃金法の違反について行政指導を受けたとき。

ウ　労働基準監督署に上記イの是正の報告を行ったとき。

（３）本契約に基づく業務の一部を他の者に行わせようとする場合及び派遣労働者を関わらせようとする場合にあっては、最低賃金額以上の賃金の支払及び労働関係法令の遵守を誓約した者を受託者とし、その契約金額（同一の者と複数の契約を締結した場合には、その合計金額。）が200万円を超えるときは、この誓約書に準ずるものとして別に県が定める誓約書を提出させ、その写しを県に提出すること。

（４）受託者が労働関係法令を遵守していないと認めるときは、当該受託者に対し、指導その他の労働者の適正な労働条件を確保するために必要な措置を講ずること。

（５）本契約に基づく業務において、次のいずれかに該当するときに県が行う本契約の解除、違約金の請求その他県が行う一切の措置について異議を唱えないこと。

ア　県に対し、上記(2)の報告をせず、又は虚偽の報告をしたとき。

イ　最低賃金法第4条第1項の規定に違反したとして、検察官に送致されたとき。

令和　　年　　月　　日

兵庫県立　　高等学校長　様

所　在　地
名　　称
代表者職氏名
電　　話　（　　）　　－　　番
電子メール

別表（誓約事項(1)関係）

労働関係法令
(1) 労働基準法（昭和22年法律第49号）
(2) 労働組合法（昭和24年法律第174号）
(3) 最低賃金法（昭和34年法律第137号）
(4) 労働安全衛生法（昭和47年法律第57号）
(5) 雇用の分野における男女の均等な機会及び待遇の確保等に関する法律（昭和47年法律第113号）
(6) 労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和60年法律第88号）
(7) 短時間労働者及び有期雇用労働者の雇用管理の改善等に関する法律（平成5年法律第76号）
(8) 労働契約法（平成19年法律第128号）
(9) 健康保険法（大正11年法律第70号）
(10) 厚生年金保険法（昭和29年法律第115号）
(11) 雇用保険法（昭和49年法律第116号）
(12) 労働保険の保険料の徴収等に関する法律（昭和44年法律第84号）

様式８（第５の 16 関係）
（誓約書）

誓　　約　　書

下記１の契約（以下「本契約」という。）に係る契約保証金の免除について、下記２の事項を誓約する。

記

１　契約名

兵庫県立神崎高等学校普通科教育用コンピュータ一式賃借

２　誓約事項

⑴　次の契約について、すべて誠実に履行したこと。

契約履行年月日	契　約　名	契約金額	契約の相手方

⑵　本契約についても、誠実に履行すること。

⑶　上記⑴及び⑵に違反したときには、本契約の解除、違約金の請求その他県が行う一切の措置について異議を述べないこと。

令和　　年　　月　　日

兵庫県立　　高等学校長　様

所　在　地
名　　称
代表者職氏名
電　　話
電子メール

様式８（第５の 16 関係）
（誓約書）

［留意事項］
誓約書の２⑴には、過去２年間（注１）に国（公社・公団を含む。）、地方公共団体その他知事が指定する公共的団体（注２）とその契約と種類（注３）及び規模（注４）をほぼ同じくする（注５）契約を数回以上（注６）にわたって締結し、履行したもののみを記入すること。また、その契約実績が確認できる書類（契約書（変更契約書を含む。）の写し、履行実績証明書等のいずれか）を添付すること。ただし、入札参加申込時等に提出したものと同一のものであれば添付不要とする。

（注１）「過去２年間」とは、契約を締結しようとする日を起算日とする。
（注２）「その他知事が指定する公共的団体」とは、兵庫県住宅供給公社、兵庫県道路公社、兵庫県土地開発公社又は国若しくは兵庫県が資本金、基本金その他これらに準ずるものの２分の１以上を出資している一般社団法人及び一般財団法人並びに株式会社をいう。
（注３）「種類」とは、次表のとおりとする。（例示）

区　分	種　　類
物品関係役務の調達契約	・製造の請負 ・物件の買入れ、借入れ ・測量・建設コンサルタント等業務以外の役務の調達

（注４）「規模」とは、契約金額をいう。ただし、長期継続契約による場合は、契約書に月額の記載があるときは、契約金額に 12 を乗じて得た金額とし、月額の記載がないときは、契約総額を契約月数で除した額に 12 を乗じて得た金額を指すものとする。
（注５）「ほぼ同じくする」とは、契約予定金額の７割に相当する金額以上のものをいう。
（注６）「数回以上」とは、２回以上をいう。

兵庫県情報セキュリティ対策指針

第１章　情報セキュリティ対策基本方針

（目的）

第１条　この指針は、兵庫県（以下「県」という。）の情報資産を適切に保持するため、情報システムの信頼性及び安全性の確保に必要な情報セキュリティ対策の基本方針と具体的な対策を講ずるに当たっての基準を定めるものとする。

（定義）

第２条　この指針の用語の定義は、当該各号に定めるところによる。

(1) 情報資産　情報システムの開発、運用、利用等に係るすべての電磁的に記録されたデータをいう。

(2) 情報セキュリティ対策　情報資産の完全性、可用性、機密性を保持し、適正な利用を確保することをいう。

(3) 情報システム　コンピュータ、通信機器、通信回線及び記録媒体で構成され、業務に関する情報処理を行う仕組みをいう。

(4) ネットワーク　複数のコンピュータを通信回線により、互いに資源を共有することができるように結合させた仕組みをいう。

(5) サーバ　情報システムを構成する機器のうち、特定のサービスを提供するコンピュータをいう。

(6) ＩＤ　情報システムの利用者を識別するための記号をいう。

(7) ＩＤカード　情報システムの利用者を識別するための磁気又はＩＣカードをいう。

(8) パスワード　情報システムの利用者であることを確認するために使用される記号をいう。

(9) 不正アクセス　情報システムを利用する権限のない者が不正な手段でこれを利用することをいう。

(10) バックアップ　データの滅失、き損に備えた複製をいう。

(11) コンピュータウィルス　情報システムの正常な動作を意図的に妨げるプログラムをいう。

(12) 外部サービス　一般の事業者等の県以外の組織が情報システムの一部又は全部の機能を提供するクラウドサービス、ホスティングサービス、ハウジングサービス、ソーシャルメディアサービス等のサービスをいう。

（対象範囲）

第３条　この指針は、県の各機関が構築・運用するすべての情報システムを対象とする。

２　前項の機関の範囲は、知事、議会、教育委員会、選挙管理委員会、人事委員会、監査委員、労働委員会、収用委員会、海区漁業調整委員会、内水面漁場管理委員会並びに公営企業及び病院事業の管理者とする。

３　この指針は、前項の機関のすべての職員（臨時職員、再任用職員、非常勤職員等を含む。）及び前項の機関から情報システムの開発・運用を委託された外部委託事業者等（以下「利用者」という。）に適用する。

（情報資産の分類）

第４条　情報セキュリティ対策は、情報資産をその内容に応じて分類し、その重要度に応じて行うものとする。

（情報資産への脅威）

第５条　情報セキュリティ対策は、兵庫県が保有する情報資産を次の各号に掲げる脅威から的確かつ効率的に保護することを目的とする。

(1) 情報システムへの不正アクセス、不正操作、利用者による意図しない操作、コンピュータウィルスの頒布、過剰な負荷をかける行為等によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難、情報システムの中断及び停止等。

(2) 利用者による記録媒体の持出、規定外の端末接続等によるデータやプログラムの漏洩、流出等。

(3) 地震、落雷、火災等の災害並びに事故、故障等による情報システムの損傷、中断及び停止。

（情報セキュリティ対策）

第６条　前条で示した脅威から情報資産を保護するために、次の各号に掲げる対策を講ずるものとする。

(1) 物理的セキュリティ対策

情報システムを構成する機器及びこれらの機器・設備を設置する施設の入退室管理等情報システムの設置に伴う安全性を確保するために必要な対策を講ずる。

(2) 人的セキュリティ対策

情報システムの利用者の責務を明らかにするとともに情報セキュリティ対策に関する研修や啓発を行うなど情報システムの適正な利用を確保するために必要な対策を講ずる。

(3) 技術的セキュリティ対策

情報システムへの不正アクセスの防止、コンピュータウィルス対策、情報システムにおけるアクセス制御等の情報システムの開発及び運用における技術的信頼性を確保するために必要な対策を講ずる。

(4) 運用面の対策

情報システムの監視、指針の遵守状況の確認、緊急事態に対応した危機管理等により情報システムの運用面における信頼性を確保し、この指針を効果的に運用するために必要な対策を講ずる。

（情報システム全体の強靭性の向上）

第７条　情報セキュリティの強化のため、情報システム全体に対し次の各号に掲げる

対策を講じるものとする。

(1) 住民情報の流出を防ぐため、個人番号（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年号外法律第27号）第２条第５項に規定する個人を特定する番号）を利用する業務システムにおいては、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先を除き、原則として、他の領域との通信を遮断する対策を講じるものとする。

(2) ＬＧＷＡＮ（高度なセキュリティを確保した上で各地方公共団体の内部システムを相互接続する行政専用のネットワーク）に接続された業務システムにおいては、インターネットに接続された業務システムとの通信経路を遮断し、両システム間で通信する場合には、インターネットメール本文のテキスト化、端末への画面転送等の無害化処理を実施するものとする。

(3) インターネットに接続された業務システムにおいては、県及び県内市町のインターネットとの通信を集約した兵庫県情報セキュリティクラウドを活用した高度な情報セキュリティ対策を行うものとする。

(4) 業務の効率性・利便性向上のため、主たる職員端末、業務システム、重要な情報資産等をインターネットに接続して利用する場合は、事前に外部による確認を実施し、必要な情報セキュリティ対策を講じた上で、利用中も定期的に外部監査を実施するものとする。

（情報セキュリティ対策統括者）

第８条　この指針に基づき、全庁的な情報セキュリティ対策を統括する責任者として、情報セキュリティ対策統括者（以下「統括者」という。）を置く。

２　統括者には企画部デジタル改革課システム企画官をもって充てる。

３　統括者は、情報資産の流出、漏えい、改ざん並びに情報システムの障害、誤動作等の事故（以下「事故等」という。）に対処するための体制を整備し、役割を明確化するものとする。

４　前項に掲げる体制に関し必要な事項については別に定める。

（情報セキュリティ対策委員会）

第９条　県における情報セキュリティ対策を円滑に推進するため、情報セキュリティ対策委員会（以下「委員会」という。）を置く。

２　委員会の委員長は統括者をもって充てる。

３　委員会は、情報セキュリティ対策の推進方策や指針の見直し等について協議、調整を行う。

４　その他委員会の運営に関し必要な事項については別に定める。

（運用管理者の責務）

第10条　この指針に基づき、情報システムの適正な運用を図るために、各情報システムに情報セキュリティ対策の運用管理者（以下「運用管理者」という。）を置く。

２　運用管理者には、当該情報システムの業務主管課室長をもって充てる。ただし、当該情報システムにおいて他の業務管理者が定められている場合はこの限りではない。

３　運用管理者は、当該情報システムの適正な運用を図るために必要な情報セキュリティ対策の実施手順（システム運用管理要綱）を策定しなければならない。
４　運用管理者は、この指針及び実施手順の遵守状況を点検チェックシートにより適宜点検し、これらの実効性が保たれるよう必要な措置を講じなければならない。

（利用責任者の責務）
第11条　情報システムの適正な利用を確保するため、各所属に情報システムの利用責任者（以下「利用責任者」という。）を置く。
２　利用責任者には次の各号に掲げる者をもって充てる。
(1) 本庁においては課室長とする。
(2) 地方機関においては地方機関の長、教育機関の長、県立学校の校長とする。ただし、県民局及び県民センターにあっては室等の長及び事務所の長等とする。
３　利用責任者は、各所属においてこの指針及び運用管理者が定める実施手順が遵守されるよう必要な措置を講じなければならない。

（利用者の責務）
第12条　利用者は、この指針及び実施手順を遵守し、情報システムを適正に利用しなければならない。

（評価及び見直し）
第13条　運用管理者は、この指針を踏まえた情報セキュリティ対策の遵守状況について定期的に監査し、その結果を統括者に報告しなければならない。
２　統括者は、委員会での協議を踏まえ、必要に応じて指針の見直しを行わなければならない。

第２章　情報セキュリティ対策基準

第１節　物理的セキュリティ対策

（機器の設置）
第14条　運用管理者は、情報システムの機器の設置について、次の各号に掲げる措置を講じなければならない。
(1) 火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう固定する等の措置を講ずること。
(2) 情報システムを設置する事務室への不正な侵入や盗難を防止するため施錠の徹底等必要な措置を講ずること。
(3) 利用者以外の者が容易に操作できないように、利用者のＩＤ及びパスワードの設定等の措置を講ずること。
(4) ディスプレイ装置、配線等から放射される電磁波による情報の外部への漏えいを防止する措置を講ずること。

(5) 当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備えつけること。
(6) 落雷等による過電流に対して機器を保護するために必要な措置を講ずること。
(7) 機器の配線に当たっては、損傷等を受けることがないよう必要な措置を講ずること。

（情報システム室の設置管理）
第15条　運用管理者は、重要な情報システムの設置、運用及び管理を行うための施設（以下「情報システム室」という。）を設置する場合は、次の各号に掲げる対策を講じなければならない。
(1) 情報システム室には、耐震対策、防火対策、防犯対策等の措置を講ずること。
(2) 情報システム室の入退室はあらかじめ許可した者のみとし、ビデオカメラによる監視装置、カード、指紋認証等による入退室管理又は入退室管理簿の記載を行うこと。
(3) 情報システム室へ機器等を搬入する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について確認を行うこと。
(4) 情報システム室内の機器の配置は、緊急時に利用者が円滑に避難できるように配慮すること。
２　情報システム室に入室する者は、身分証明書等を携帯し、運用管理者の指定する担当職員の求めに従い提示しなければならない。
３　情報システム室に機器等を設置しようとする者は、当該情報システム室を設置する運用管理者の指示に従わなければならない。
４　運用管理者は、民間事業者等他の機関が管理する施設に情報システムを設置して運用を委託するときは、次の各号に掲げる事項を遵守しなければならない。
(1) 当該施設が第１項に規定する対策が講じられていることを確認すること。
(2) 当該施設におけるセキュリティ対策の実施状況について定期的に監査すること。
(3) その他、この指針で定める対策基準に基づき適正な外部委託の管理を行うこと。

第２節　人的セキュリティ対策

（情報資産の管理）
第16条　情報資産の管理に当たって、利用者は次の各号に掲げる事項を遵守しなければならない。
(1) データのき損、滅失等に備えるため、保管するデータのバックアップを定期的に作成すること。
(2) 重要な情報資産はパスワードを施すなど適切な管理を行うこと。
(3) 退庁時及び長時間離席する場合は、使用する端末等の電源を切ること。
(4) 運用管理者の許可を得ず、情報システムで処理するデータ及びその複製を定められた場所から移動させないこと。
(5) その他、自己の管理する情報が他に流出しないよう保護すること。

（記録媒体の管理等）

第17条　情報資産をハードディスク、USBメモリ等の記録媒体で管理する場合は、次の各号に掲げる措置を講じなければならない。

(1) 取り出し可能な記録媒体を、盗難や損傷の防止のために適切な管理を行うこと。また、個人情報等が記録された機密情報を含む当該記録媒体を定められた場所から持ち出す場合は、運用管理者または利用責任者の許可を得ることとし、データの暗号化、パスワードによる保護、施錠できる搬送容器の使用、追跡可能な移送手段の利用等の措置を講じなければならない。

(2) 記録媒体は、防犯、耐火、耐熱、耐水及び耐湿対策等を講じた施錠可能な場所に保管し、管理簿を設けるなど適切な管理を行うこと。

(3) 記録媒体が不要となった場合は、当該媒体に含まれる情報は、記録媒体の初期化など情報を復元できないように消去を行ったうえで廃棄すること。

２　運用管理者は、記録媒体、機器等の廃棄、返却等を行う場合、記録媒体、機器内部の記憶装置等から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（利用禁止行為）

第18条　利用者は、情報システムの利用について次の各号に掲げる行為を行ってはならない。

(1) 業務に関連しない目的で情報システムを利用すること。

(2) 法令又は公序良俗に反した利用を行うこと。

(3) 他の利用者又は第三者の著作権、人権及びプライバシーを侵害するおそれのある利用を行うこと。

(4) 情報の改ざん、き損及び滅失並びに虚偽の情報提供を行うこと。

(5) 通信を阻害する行為及び情報資産に損害又は不利益を及ぼす利用を行うこと。

２　運用管理者は、前項に該当する利用が行われていると認める場合は、当該利用者に対して情報システムの利用を停止することができる。

（生成AIシステムの利用）

第18条の２　利用者は、生成AI（人工的な方法により学習、推論、判断等の知的機能を備え、かつ、質問その他のコンピュータに対する入力情報に応じて当該知的機能の活用により得られた文章、画像、音声等の結果を自動的に出力するよう作成されたプログラム及び当該プログラムと連携して動作するプログラムをいう。以下同じ。）を用いた情報システム（無償で提供される外部サービスを含む。以下「生成AIシステム」という。）の利用について、前条第１項の規定のほか、次の各号に掲げる事項を遵守しなければならない。

(1) 運用管理者が利用者を定める生成AIシステムを除き、利用について運用管理者又は利用責任者（無償で提供される外部サービス等で運用管理者及び利用責任者の定めのない場合は、第11条第２項各号に掲げる者）の許可を得ること。

(2) 安全性が確認されたものとして統括者が許可した生成AIシステムを除き、入力情報に非公開情報（個人情報その他の情報公開条例（平成12年兵庫県条例第６号）第

６条に規定する非公開情報をいう。以下同じ。）を含めないこと。
(3) 生成AIから出力された結果の正確性を確認すること。

（ＩＤ及びパスワードの管理）
第19条　利用者は、自己の保有するＩＤ及びパスワードに関し、次の各号に掲げる事項を遵守しなければならない。
(1) 他の利用者のＩＤは使わないこと。
(2) パスワードは十分な長さとし、文字列はアルファベット、数字及び記号を混在させるなど容易に推定できないものとすること。
(3) パスワードは定期的に変更し、古いパスワードの再利用はしないこと。
(4) パスワードを秘密にし、パスワードの照会等には一切応じないこと。
(5) パスワードの盗用や漏えいがあった場合は、直ちに利用責任者に連絡すること。
(6) その他、ＩＤ及びパスワードの適正な管理を行うこと。
２　利用者はＩＤカードの利用について、次の各号に掲げる事項を遵守しなければならない。
(1) ＩＤカードを利用者間で共有しないこと。
(2) ＩＤカードを、カードの読み取り装置又は端末に常時挿入しないこと。
(3) ＩＤカードを紛失した場合には、速やかに利用責任者に通報し、指示を仰ぐこと。

（教育・訓練）
第20条　統括者は、すべての職員がこの指針について理解を深め、遵守を徹底するよう、情報セキュリティ対策に関する研修の実施や普及啓発を行わなければならない。
２　運用管理者は、情報システムに不測の事態が発生した場合に備えた訓練を計画的に行わなければならない。

（事故等の報告）
第21条　利用者は、事故等を発見した場合には、直ちに利用責任者に報告し、その指示に従い必要な措置を講じなければならない。
２　利用責任者は、事故等の報告を受けた場合は、直ちに当該事故等の内容を運用管理者に報告しなければならない。

（外部委託に関する管理）
第22条　運用管理者は、情報システムの開発・保守運用を民間事業者等に委託する場合は、この指針を踏まえ当該外部委託事業者が遵守すべき事項を明記した契約を締結しなければならない。
２　運用管理者は、個人情報取扱事務その他の個人情報を取り扱う事務を外部委託事業者に委託しようとするときは、当該外部委託事業者との契約書に、個人情報取扱特記事項（「個人情報を取り扱う事務の委託に伴う措置について（平成９年11月21日付け文第294号知事公室長通知）」）を規定しなければならない。
３　運用管理者は、外部委託事業者との契約書には、この指針及び実施手順が遵守され

なかった場合の損害賠償等の規定を定めなければならない。
4　運用管理者は、外部委託事業者の選定時において、この指針に定める情報資産の安全管理措置と同等の措置が講じられているかを確認しなければならない。
5　外部委託事業者は、情報システムの開発・保守運用の外部委託において再委託（三次委託以降を含む。以下「再委託等」という。）が行われる場合、再委託先（三次委託以降の委託先を含む。以下「再委託事業者等」という。）の名称、業務範囲、再委託等を行う必要性等、県が求める項目を書面で運用管理者に提出し、再委託等の許可を求めなければならない。
6　運用管理者は、外部委託事業者から前項に規定する再委託等の許可を求める書面が提出された場合、その内容を確認し、再委託等に問題がないと認める場合には承認できるものとする。
7　外部委託事業者は、前２項の手続きにより再委託等が承認された場合、再委託事業者等の行為について、県に対し全ての責任を負うものとする。
8　外部委託事業者は、この指針で定める運用管理者の遵守事項（再委託事業者等への対応を含む）について、その実現のために協力しなければならない。
9　運用管理者は、外部委託事業者からこの指針の遵守状況（再委託事業者等の遵守状況を含む）について定期的な報告を受けるなど、適切な監督を実施し、支障を認めた場合は必要な措置を講じなければならない。
10　運用管理者は、外部委託事業者及び再委託事業者等とのデータの受け渡しに係る内容、日付等を記録しなければならない。
11　運用管理者は、外部委託事業者及び再委託事業者等の責任者や業務に携わる社員の名簿を作成するとともに、その作業場所を特定しなければならない。
12　運用管理者は、身分証明書の提示を外部委託事業者及び再委託事業者等に求めるなどにより、契約で定められた資格を有するものが作業に従事しているか確認を行わなければならない。
13　運用管理者は、外部委託事業者及び再委託事業者等の従業員に対する教育が実施されているかを確認しなければならない。

第３節　技術的セキュリティ対策

（アクセス記録の取得等）
第23条　運用管理者は、各種アクセス記録及び情報セキュリティ対策に必要な記録をすべて取得し、１年以上の期間を定めて、保存しなければならない。
2　前項に掲げる以外の情報については、その重要度に応じて期間を設定し、バックアップを作成しなければならない。
3　運用管理者は、定期的にアクセス記録等を分析、監視しなければならない。
4　運用管理者は、アクセス記録等が窃取、改ざん、消去されないように必要な措置を講じなければならない。

（情報システムの入出力データ）
第24条　運用管理者は、当該情報システムに入力されるデータの正確性を確保するため

の対策を講じなければならない。
2　運用管理者は、利用者又は利用者以外の者の故意又は過失による誤ったデータの入力により情報が改ざんされるおそれがある場合、これを検出する手段を講じなければならない。また、改ざんの有無を検出し、必要な場合は情報の修復を行う手段を講じなければならない。
3　運用管理者は、情報システムから出力されるデータが、正しく情報処理され、出力されることを確保しなければならない。

（電子署名・暗号化）
第25条　運用管理者は、機密情報及び重大な情報については、機密性を保護するために暗号化しなければならない。
2　暗号化に係る運用管理については別に定める。

（機器構成の変更）
第26条　運用管理者は、情報システムの機器に業務上必要でないプロトコル（通信手順）を設定してはならない。
2　利用者は、端末の改造及び機器の増設・交換を行ってはならない。
3　利用者は、運用管理者の許可なく、その使用する端末にＩＤの追加、共有データの設定、ソフトウェアの追加等の設定変更を行ってはならない。

（利用者の管理）
第27条　運用管理者は、情報システムの利用者の登録、変更、抹消等登録情報の管理及び異動、退職した職員等のＩＤ及びパスワードの管理等利用者を適正に管理しなければならない。

（情報システムにおけるアクセス制御）
第28条　運用管理者は、情報システムにおけるアクセス制御について次の各号に掲げる事項を遵守しなければならない。
(1) アクセス権限の許可は必要最小限にすること。
(2) 不正アクセスを防止するため、ユーザ認証、論理的なネットワークの分割、ファイアウォール（組織内の情報通信機器や端末に外部からの侵入を防ぐ目的で設置してあるセキュリティシステム）の設置等の適切なネットワーク経路制御を講ずること。
(3) アクセス方法等は利用者の真正性が確保できるものにすること。
(4) 接続した情報通信機器についてセキュリティに問題が認められ、情報システムの情報資産に脅威が生じることが想定される場合には、速やかに当該情報通信機器を内部ネットワークとの接続から物理的に遮断すること。

（外部ネットワークとの接続）
第29条　県の情報システムと県以外の機関が管理する情報システム（以下「外部ネットワーク」という。）との接続については、次の各号に掲げる事項を遵守しなければな

らない。
(1) 不正アクセスを防止するためのファイアウォールの設置や利用者の認証、論理的なネットワークの分割等適切なネットワーク経路制御を講ずること。
(2) 外部から情報システムにアクセスする場合は、ユーザ認証、ファイアウォールの設置等のネットワーク上の制御を講ずること。
(3) 外部ネットワークとの接続により情報システムの運用及び情報資産の保持に支障が生じるおそれがある場合は、直ちに当該情報システムと外部ネットワークとの接続を物理的に遮断すること。

（情報システムの開発）
第30条　運用管理者は、情報システムの開発について次の各号に掲げる事項を実施しなければならない。
(1) 情報システムの開発、保守等に関する事故及び不正行為に係るリスク（危険性）の評価を行うこと。
(2) プログラム、設定等のソースコードを整備すること。
(3) セキュリティの確保に支障が生じるおそれのあるソフトウェアは使用しないこと。
(4) 情報システムの開発及び保守に係る記録を作成するとともに、運用、管理等に必要な説明書等の書類は定められた場所へ保管すること。
(5) 不要になった利用者ＩＤ、パスワード等は速やかに抹消すること。

（情報システムの調達）
第31条　運用管理者は、情報システムの機器及びソフトウェアの調達に伴う仕様書の作成については、情報セキュリティ対策上支障が生じるおそれのある内容を記載しないようにしなければならない。
２　運用管理者は、機器及びソフトウェアを調達する場合は、当該製品の安全性及び信頼性を確認しなければならない。

（ソフトウェアの保守及び更新）
第32条　運用管理者は、独自開発ソフトウェア及びＯＳ等を更新し又は修正プログラムを導入する場合は、不具合及び他のシステムとの適合性の確認を行い、計画的に更新し又は導入しなければならない。
２　運用管理者は、情報セキュリティに重大な影響を及ぼす不具合に関して常に情報を収集し、発見した場合は、修正プログラムの導入等速やかな対応を行わなければならない。

（コンピュータウィルス対策）
第33条　運用管理者は、コンピュータウィルスによる情報システムの安全性を確保するため、次の各号に掲げる事項を実施しなければならない。
(1) 外部のネットワークからデータを取り入れる際には、ファイアウォール、メールサーバ等においてウィルスチェックを行いシステムへの侵入を防止すること。

(2) 外部のネットワークへデータを送信する際にも、前号と同様のウィルスチェックを行い、外部へのコンピュータウィルスの拡散を防止すること。
(3) コンピュータウィルス情報について利用者に対する注意喚起を行うこと。
(4) 端末においてウィルス対策用のソフトウェアを導入すること。
(5) ウィルスチェック用のパターンファイルは常に最新のものに保つこと。
(6) コンピュータウィルスに対する修正プログラムの入手に努め、サーバ及び端末に速やかに適用すること。
(7) コンピュータウィルスの感染のおそれの少ないソフトウェアの選定を行うこと。

2　利用責任者は、利用者がコンピュータウィルスを発見した場合、又はコンピュータウィルスにより障害が生じたと認められる場合は、直ちに運用管理者に連絡し、その指示に従わなければならない。

3　利用者は、コンピュータウィルスによる被害を防止するため、次の各号に掲げる事項を遵守しなければならない。
(1) 差出人が不明な電子メールや不審なファイルが添付された電子メールを受信した場合は開封せず、直ちに削除すること。
(2) 添付ファイルのあるメールを送信する場合は、ウィルスチェックを行うこと。
(3) 外部から入手したデータは、必ずウィルスチェックを行うこと。
(4) 万一のコンピュータウィルス被害に備えるため、データのバックアップを作成すること。
(5) 運用管理者が提供するウィルスチェック用のパターンファイルは常に最新のファイルに更新すること。
(6) 運用管理者が提供するコンピュータウィルス情報を常に確認すること。

（不正アクセス対策）

第34条　運用管理者は、不正アクセスを防止するため、次の各号に掲げる対策を講じなければならない。
(1) 使用終了又は使用される予定のないポート（ネットワーク上のサーバがサービスを区別するために使っている番号）を長時間空けた状態のままにしないこと。
(2) 情報通信機器及び端末上の不要なＩＤは速やかに削除すること。
(3) ソフトウェアの不備に伴うセキュリティホールに対しては、速やかに修正プログラムを適用すること。
(4) 不正アクセスによるウェブページの改ざんを防止するために、ウェブページ改ざんを検出し、運用管理者へ通報する設定を講ずること。
(5) 重要な情報システムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査すること。
(6) 不正アクセスを受けるおそれが認められる場合には、情報システムの停止を含む必要な措置を講ずること。

2　運用管理者は、不正アクセスを受けた場合は、直ちに統括者及び関係機関に連絡を行い、情報システムの復旧等必要な措置を講じなければならない。

3　利用責任者は、不正アクセスを受けた場合は、直ちに運用管理者に連絡し、その指示に従わなければならない。

（セキュリティ情報の収集）

第35条　統括者は、情報セキュリティに関する情報を積極的に収集し、運用管理者や利用責任者等に速やかに周知し、必要な措置を講じなければならない。

２　統括者は、前項の情報を定期的に取りまとめ、関係部局等に通知するとともに、この指針の改定につながる情報については委員会に報告しなければならない。

（無線ＬＡＮの対策）

第36条　運用管理者は、無線ＬＡＮの利用に当たり、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。

２　運用管理者は、無線ＬＡＮに対する情報の盗聴等を防ぐため、ハードウェア及びソフトウェアの迅速な更新、定期的な監査等を実施しなければならない。

（在宅勤務等の対策）

第37条　運用管理者は、在宅勤務、職場外勤務等により、外部から県内部の業務システムにアクセスするためのシステム（以下「在宅勤務等システム」という。）を構築又は利用する場合、通信途上の盗聴を防ぐために暗号化、利用経路の閉域化等の対策を講じなければならない。

２　運用管理者は、在宅勤務等システムの利用を認める場合、利用者の本人確認を行う機能を確保しなければならない。

３　運用管理者は、外部からアクセスするために利用するモバイル端末を貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

４　利用者は、在宅勤務等システムを利用する場合、運用管理者の許可を得なければならない。

５　その他在宅勤務等システムに関し必要な事項については別に定める。

（外部サービス利用の対策）

第38条　運用管理者は、外部サービスを利用しようとする場合は、利用目的及び業務範囲を明確にするとともに、取り扱う情報の内容に応じ、情報の保存場所、裁判管轄、準拠法等のリスクの対策を検討した上で、外部サービスの提供者を選定しなければならない。

２　運用管理者は、外部サービスにおいて非公開情報を取り扱う場合は、あらかじめ統括者の許可を得なければならない。この場合において、外部サービスの提供者が不特定多数の利用者に対して提供する画一的な約款、規約等への同意のみで利用が可能となる外部サービスでは、原則として非公開情報を取り扱ってはならない。

３　運用管理者は、利用する外部サービスの情報セキュリティ対策について、外部サービスの提供者との責任の分担を定め、その実施状況を定期的に確認しなければならない。

４　統括者は、県の各機関における外部サービスの利用状況を把握し、必要な措置を講じなければならない。

５　その他外部サービスの利用に関し必要な事項については別に定める。

（生成AIシステムの対策）

第38条の２　運用管理者は、生成AIシステムの導入及び運用をするに当たり、入力情報が運用管理者の許可なく生成AIの学習に用いられない環境の整備その他情報セキュリティの確保のために必要な措置を講じなければならない。

第４節　運用面の対策

（情報システムの監視）

第39条　運用管理者は、情報システムの円滑な運用を確保するため、情報システムを定期的に監視し、障害が起きた際は速やかに対応しなければならない。

２　運用管理者は、外部と常時接続するシステムについては、ネットワーク侵入監視装置を設置し、24時間監視を行わなければならない。

３　運用管理者は、情報システム内部において、適正なアクセス制御を行い、運用状況について監視を行わなければならない。

４　運用管理者は、監視した結果を正確に記録するとともに、消去や改ざんをされないよう必要な措置を施し、安全な場所に保管しなければならない。

（指針の遵守状況の確認）

第40条　利用者は、この指針に違反した場合及び違反の発生を確認した場合は、直ちに利用責任者に報告を行わなければならない。

２　利用責任者は、この指針の遵守状況及び情報資産の管理状況について常に確認を行い、支障を認めた場合には速やかに運用管理者に報告しなければならない。

３　運用管理者は、情報システムにおけるこの指針の遵守状況及び情報資産の管理状況について定期的に確認を行い、支障を認めた場合には、迅速かつ適切に対処しなければならない。

（緊急時対応計画等）

第41条　運用管理者は、情報資産への侵害が発生した場合に備えて、あらかじめ関係機関との連絡体制や復旧対策など緊急時対応計画を策定しなければならない。

２　利用責任者は、情報資産への侵害発生及び侵害発生の危険性を発見した場合は、事案の内容、原因、被害の状況等を速やかに運用管理者に報告しなければならない。

３　運用管理者は、情報資産への侵害に起因して、住民に重大な被害が生じるおそれがある場合、又は行政の運営に重大な支障が生じる場合は、統括者に直ちに報告するとともに、関係機関に速やかに連絡しなければならない。

４　運用管理者は、情報システムに障害が発生し、情報資産の保持のために情報システムの停止がやむを得ないと認められる場合は、ネットワークを切断することができる。

５　運用管理者は、各種セキュリティに関する事案の詳細な調査を行うとともに、再発防止計画を策定しなければならない。

（法令遵守）

第42条　利用者は、情報システムの運用については、次の各号に掲げる法令を遵守し、これに従わなければならない。

(1) 不正アクセス行為の禁止等に関する法律(平成11年法律第128号)
(2) 著作権法(昭和45年法律第48号)
(3) 個人情報の保護に関する法律（平成15年法律第57号)
(4) その他情報セキュリティ対策に関する法令

附　則

この指針は、平成15年３月４日から適用する。

附　則

この指針は、平成15年４月１日から適用する。

附　則

この指針は、平成16年４月１日から適用する。

附　則

この指針は、平成17年４月１日から適用する。

附　則

この指針は、平成18年４月１日から適用する。

附　則

この指針は、平成20年４月１日から適用する。

附　則

この指針は、平成23年４月１日から適用する。

附　則

この指針は、平成25年４月１日から適用する。

附　則

この指針は、平成26年４月１日から適用する。

附　則

この指針は、令和２年４月１日から適用する。

附　則

この指針は、令和３年４月１日から適用する。

附　則

この指針は、令和３年８月10日から適用する。

附　則

この指針は、令和３年９月１日から適用する。

附　則

この指針は、令和４年４月１日から適用する。

附　則

この指針は、令和４年７月20日から適用する。

附　則

この指針は、令和５年７月18日から施行する。

兵庫県教育情報セキュリティ対策基準

第１節　趣旨

第１条　この対策基準は、兵庫県教育委員会行政組織規則（昭和58年教育委員会規則第９号）第３条第３項に規定する県立学校（以下「学校」という。）における情報セキュリティを確保するため、兵庫県情報セキュリティ対策指針（平成15年政策会議決定）第２章について、特別の情報セキュリティ対策基準を定めるものである。

２　兵庫県情報セキュリティ対策指針第１章及びこの対策基準をもって兵庫県（以下「県」という。）の教育情報セキュリティポリシーとする。

第２節　対象範囲及び用語説明

（適用範囲）

第２条　教育情報セキュリティポリシーは、学校の情報資産に係る業務に携わるすべての職員を対象とする。

（情報資産の範囲）

第３条　この対策基準が対象とする情報資産は、次のとおりとする。

(1) 教育情報ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体

(2) 教育情報ネットワーク及び教育情報システムで取り扱う情報（これらを印刷した文書を含む。）

(3) 教育情報システムの仕様書及び教育情報ネットワーク図等のシステム関連文書

（用語説明）

第４条　この対策基準における用語は、次の表に掲げるとおりとする。

用語	定義
校務系情報	児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教職員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報
校務外部接続系情報	校務系情報のうち、保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報
学習系情報	児童生徒のワークシート、作品など、学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ当該情報に教職員及び児童生徒がアクセスすることが想定されている情報
教員用端末	校務系情報にアクセス可能な端末で、仮想デスクトップから校務系情報にアクセス可能な校務用端末
	学習系情報にアクセス可能な端末で、教職員のみが利用可能な指導者用端末
学習者用端末	学習系情報にアクセス可能な端末で、児童生徒が利用する端末（児童生徒が所有する端末を含む。）
校務系システム	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム

校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ及び校務用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
教育情報ネットワーク	兵庫県教育情報ネットワーク（学校からの回線で直接インターネットへ接続するものを含む。）
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ

第３節　組織体制

（最高情報セキュリティ責任者）

第５条　教育次長を最高情報セキュリティ責任者（Chief Information Security Officer、以下「CISO」という。）とする。

２　CISOは、県における全ての教育情報ネットワーク、教育情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

（統括教育情報セキュリティ責任者）

第６条　教育企画課長をCISO直属の統括教育情報セキュリティ責任者とする。統括教育情報セキュリティ責任者はCISOを補佐しなければならない。

２　統括教育情報セキュリティ責任者は、教育情報ネットワーク及び教育情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

３　統括教育情報セキュリティ責任者は、教育情報ネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

４　統括教育情報セキュリティ責任者は、県において所有している教育情報システムについて、教育情報セキュリティポリシーの遵守に関する意見の集約を行う。

５　統括教育情報セキュリティ責任者は、教育情報セキュリティ管理者、教育情報システム管理者及び教育情報システム管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

６　統括教育情報セキュリティ責任者は、県の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISOの指示に従い、CISOが不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

７　統括教育情報セキュリティ責任者は、県の共通的な教育情報ネットワーク、教育情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

８　統括教育情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム管理者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

９　統括教育情報セキュリティ責任者は、緊急時にはCISOに早急に報告を行うとともに、回復のための対策を講じなければならない。

（教育情報セキュリティ責任者）

第７条　教職員人事課長を教育情報セキュリティ責任者とする。

２　教育情報セキュリティ責任者は、教職員に対する教育、訓練、助言及び指示を行う。
３　教育情報セキュリティ責任者は、教育情報セキュリティ管理者から報告を受けた情報セキュリティインシデントについて適切な措置を講じる。

（教育情報セキュリティ管理者）
第８条　校長を教育情報セキュリティ管理者とする。
２　教育情報セキュリティ管理者は、当該学校の情報セキュリティ対策に関する権限及び責任を有する。
３　教育情報セキュリティ管理者は、当該学校の情報セキュリティ実施手順の策定及び維持・管理を行う。
４　教育情報セキュリティ管理者は、当該学校において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、CISO及び統括教育情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

（教育情報システム管理者）
第９条　県立総合教育センター長を教育情報システム管理者とする。
２　教育情報システム管理者は、所管する教育情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
３　教育情報システム管理者は、所管する教育情報システムにおける情報セキュリティに関する権限及び責任を有する。
４　教育情報システム管理者は、所管する教育情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（教育情報システム担当者）
第10条　県立総合教育センター情報教育研修課長を教育情報システム担当者とする。
２　教育情報システム担当者は、教育情報システム管理者の指示等に従い、教育情報システムの開発、設定の変更、運用、更新等の作業を行う。

（学校教育情報セキュリティ・システム担当者）
第11条　教育情報セキュリティ管理者は、当該学校の教職員の中から学校教育情報セキュリティ・システム担当者を指名する。
２　学校教育情報セキュリティ・システム担当者は、教育情報セキュリティ管理者の指示に従い、学校における教育情報システムの導入・管理・運用等を補助する。

（教育情報セキュリティ対策委員会）
第12条　学校の情報セキュリティ対策を統一的に行うため、県で設置する教育情報セキュリティ対策委員会（以下「対策委員会」という。）において、この対策基準等、情報セキュリティに関する重要な事項を決定する。

（学校教育情報セキュリティ・システム委員会）
第13条　学校の教育情報ネットワーク、教育情報システム等の運用及びそこで取り扱う情報資産の管理を適切に行うため、各学校に学校教育情報セキュリティ・システム委員会を設置する。

（情報セキュリティに関する統一的な窓口の設置）
第14条　CISOは、情報セキュリティの統一的な窓口の機能を有する組織（以下「情報セキュリティに関する統一的な窓口」という。）を整備し、情報セキュリティインシデントについて学校等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

２　教育企画課は、CISOによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係者及び学校等に提供する。
３　教育企画課は、情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。
４　教育企画課は、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

第４節　情報資産の分類と管理方法

（情報資産の分類）
第15条　学校における情報資産は、機密性、完全性及び可用性を踏まえ、セキュリティ侵害が及ぼす影響の大きさにより、次の表に揚げるとおり重要性に基づいて分類し、必要に応じて取扱制限を行うものとする。

分類	分類基準
重要性Ⅰ	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼすもの（秘匿情報）
重要性Ⅱ	セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼすもの（保護情報）
重要性Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼさないもの（公開情報）

（情報資産の管理）
第16条　教育情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。
２　情報資産が複製又は伝送された場合には、複製等された情報資産も前条の分類に基づき管理しなければならない。
３　教職員は、情報資産について、その分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。
４　教職員は、業務上必要のない情報を作成してはならない。
５　情報を作成する者は、情報の作成時に前条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
６　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。
７　学校内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。
８　学校外の者が作成した情報資産を入手した者は、前条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
９　情報資産を入手した者は、その情報資産の分類が不明な場合、教育情報セキュリティ管理者に判断を仰がなければならない。
10　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。
11　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。
12　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。
13　教育情報セキュリティ管理者及び教育情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

14　教育情報セキュリティ管理者及び教育情報システム管理者は、情報資産を記録した電磁的記録媒体を保管する場合は、書込禁止の措置を講じなければならない。
15　教育情報セキュリティ管理者及び教育情報システム管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管するよう考慮しなければならない。
16　電子メール等により重要性Ⅱ以上の情報資産を外部送信する者は、限定されたアクセスの措置設定を行わなければならない。
17　車両等により重要性Ⅱ以上の情報資産を運搬する者は、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。
18　重要性Ⅱ以上の情報資産を運搬する者は、教育情報セキュリティ管理者に許可を得なければならない。
19　重要性Ⅱ以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。
20　重要性Ⅱ以上の情報資産を外部に提供する者は、教育情報セキュリティ管理者に許可を得なければならない。
21　教育情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。
22　重要性Ⅱ以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。紙媒体が不要となった場合は、焼却、裁断、溶解等により廃棄しなければならない。
23　情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。
24　情報資産の廃棄を行う者は、教育情報セキュリティ管理者又は教育情報システム管理者の許可を得なければならない。

第５節　物理的セキュリティ

（物理的セキュリティ）
第17条　教育情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

（サーバの冗長化）
第18条　教育情報システム管理者は、校務系サーバその他の校務系情報を格納しているサーバを冗長化し、同一データを保持しなければならない。また、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。
２　教育情報システム管理者は、学習系サーバその他の学習系情報を格納しているサーバのハードディスクを冗長化しなければならない。

（機器の電源）
第19条　教育情報システム管理者は、統括教育情報セキュリティ責任者及び外部委託業者と連携し、校務系サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。
２　教育情報システム管理者は、統括教育情報セキュリティ責任者及び外部委託業者と連

携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（通信ケーブル等の配線）

第20条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部委託事業者と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、外部委託事業者から損傷等の報告があった場合、連携して対応しなければならない。

３　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

４　統括教育情報セキュリティ責任者及び教育情報システム管理者は、自ら又は教育情報システム管理者及び契約により操作を認められた外部委託事業者以外の者が配線を変更又は、追加できないように必要な措置を施さなければならない。

（機器の定期保守及び修理）

第21条　教育情報システム管理者は、重要性Ⅱ以上の情報資産を取り扱うサーバ等の機器の定期保守を実施しなければならない。

２　教育情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、教育情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するとともに、秘密保持体制の確認等を行わなければならない。

（施設外又は学校外への機器の設置）

第22条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、施設外又は学校外にサーバ等の機器を設置する場合、CISOの承認を得なければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（機器の廃棄等）

第23条　教育情報セキュリティ管理者及び教育情報システム管理者は、機器を廃棄又はリース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（管理区域の構造等）

第24条　管理区域とは、ネットワークの基幹となる機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）及び電磁的記録媒体の保管庫をいう。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部委託業者と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

３　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

４　統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしな

ければならない。

（管理区域の入退室管理等）

第25条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理区域への入退室を許可された者のみに制限し、入退室管理簿の記載による入退室管理を行わなければならない。

２　情報システム担当職員及び外部委託事業者が、管理区域に入室することを許可する場合、これらの者に身分証明書等を携帯させ、必要に応じ、その提示を求めなければならない。

３　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された情報システム担当職員等が付き添うものとし、外見上情報システム担当職員等と区別できる措置を講じなければならない。

４　統括教育情報セキュリティ責任者及び教育情報システム管理者は、重要性Ⅱ以上の情報資産を取り扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（機器等の搬入出）

第26条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム室へ搬入する機器等が、既存の情報システムに与える影響について、あらかじめ教育情報システム管理者又は外部委託業者に確認を行わせなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム室の機器等の搬入出について、情報システム担当職員等を立ち会わせなければならない。

（通信回線及び通信回線装置の管理）

第27条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、施設内の通信回線及び通信回線装置を適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

３　統括教育情報セキュリティ責任者及び教育情報システム管理者は、重要性Ⅱ以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

４　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

５　統括教育情報セキュリティ責任者及び教育情報システム管理者は、重要性Ⅱ以上の情報資産を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。

（教員用端末の管理）

第28条　教育情報セキュリティ管理者は、盗難防止のため、教員用端末の管理について、物理的措置を講じるとともに、情報資産管理ファイルをもとに、適切な管理を行わなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

２　教育情報システム管理者は、教育情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

（学習者用端末の管理）

第29条　統括教育情報セキュリティ責任者、教育情報システム管理者及び教育情報セキュリティ管理者は、児童生徒が所有するパソコン、モバイル端末を学習者用端末とする場合には、必要な対策を講じなければならない。

2　教育情報セキュリティ管理者は、盗難防止のため、教室等で利用するパソコンの管理等について物理的措置を講じるとともに、児童生徒が所有するパソコン、モバイル端末について自己管理の徹底を図らなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

3　教育情報セキュリティ管理者は、学習系システムへのログインパスワードの入力を必要とするように設定しなければならない。

4　統括教育情報セキュリティ責任者及び教育情報システム管理者は、児童生徒が学習者用端末を利用する際に不適切なサイトの閲覧を防止するための対策を講じなければならない。

5　教育情報セキュリティ管理者は、学習者用端末を校内でウェブ利用する児童生徒に対して、当該端末におけるマルウェア感染対策を講じるよう指導しなければならない。

6　教育情報セキュリティ管理者は、学校内における学習者用端末の運用ルールを策定しなければならない。

第６節　人的セキュリティ

（教職員の遵守事項）

第30条　教職員は、教育情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに教育情報セキュリティ管理者に相談し、指示を仰がなければならない。

2　教職員は、業務以外の目的で情報資産の外部への持ち出し、教育情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

3　教職員は、モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業については、次の内容を遵守しなければならない。

(1) 教職員は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、教育情報セキュリティ管理者の許可を得なければならない。

(2) 教職員は、外部で情報処理業務を行う場合には、教育情報セキュリティ管理者の許可を得なければならない。

4　教職員は、教員用端末以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用については、次の内容を遵守しなければならない。

(1) 教職員は、教員用端末以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、教育情報セキュリティ管理者の許可を得て利用することができる。

(2) 教職員は、教員用端末以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

5　教育情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

6　教職員は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を教育情報セキュリティ管理者の許可なく変更してはならない。

7　教職員は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は教育情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒

体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。
８　教職員は、職員室等において、重要度Ⅱ以上の情報資産を取り扱う際には、児童生徒を含む外部からの入室者に情報が流出することがないように、必要な対策を行わなければならない。
９　教職員は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。
10　教職員は、児童生徒に対し、学習者用端末等を活用するにあたり、適切な指導をしなければならない。

（非常勤及び臨時の教職員への対応）
第31条　教育情報セキュリティ管理者は、非常勤及び臨時の教職員に対し、採用時にこの対策基準等のうち、非常勤及び臨時の教職員が守るべき内容を理解させ、また実施及び遵守させなければならない。
２　教育情報セキュリティ管理者は、非常勤及び臨時の教職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（教育情報セキュリティポリシー等の掲示）
第32条　教育情報セキュリティ管理者は、教職員が常に教育情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（外部委託事業者に対する説明）
第33条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、教育情報セキュリティポリシー及び実施手順のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

（情報セキュリティに関する研修・訓練）
第34条　CISOは、定期的に情報セキュリティに関する研修及び訓練を実施しなければならない。

（研修計画の策定及び実施）
第35条　CISOは、教育情報セキュリティ責任者と連携し、教職員に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、対策委員会の承認を得なければならない。
２　教育情報セキュリティ責任者は、新規採用の教職員を対象とする情報セキュリティに関する研修を実施しなければならない。
３　研修は、教育情報セキュリティ管理者、学校教育情報セキュリティ・システム担当者及びその他教職員に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。
４　CISOは、毎年度１回、対策委員会に対して、教職員の情報セキュリティ研修の実施状況について報告しなければならない。

（緊急時対応訓練）
第36条　CISOは、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

（情報セキュリティインシデントの報告）
第37条　教職員は、情報セキュリティインシデントを認知した場合、速やかに教育情報セキュリティ管理者に報告しなければならない。
２　報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に報告しなければならない。
３　教育情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じてCISO及び教育情報セキュリティ責任者に報告しなければならない。

（住民等外部からの情報セキュリティインシデントの報告）
第38条　教職員は、管理対象のネットワーク及び教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、教育情報セキュリティ管理者に報告しなければならない。
２　報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に報告しなければならない。
３　教育情報セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じてCISO及び教育情報セキュリティ責任者に報告しなければならない。

（情報セキュリティインシデント原因の究明・記録、再発防止等）
第39条　統括教育情報セキュリティ責任者は、情報セキュリティインシデントについて、教育情報セキュリティ管理者、教育情報システム管理者と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISOに報告しなければならない。
２　CISOは、統括教育情報セキュリティ責任者から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

（IDの取扱い）
第40条　教職員は、自己の管理するIDに関し、次の事項を遵守しなければならない。
(1) 自己が利用しているIDは、他人に利用させてはならない。
(2) 共用IDを利用する場合は、共用IDの利用者以外が利用してはならない。
(3) その他のソフトウェア等の管理者用IDについては、教育情報セキュリティ管理者が指名するもの以外が利用してはならない。

（パスワードの取扱い）
第41条　教職員は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。
(1) パスワードは、他者に知られないように管理しなければならない。
(2) パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
(3) パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。
(4) パスワードが流出したおそれがある場合には、教育情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
(5) パスワードは定期的に又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。
(6) 仮のパスワードは、最初のログイン時点で変更しなければならない。
(7) パソコンやモバイル端末等にパスワードを記憶させてはならない。
(8) 教職員間でパスワードを共有してはならない。ただし、共用IDに対するパスワードは除く。

第７節　技術的セキュリティ

（文書サーバ及び端末の設定等）

第42条　統括教育情報セキュリティ責任者は、教職員が使用できる文書サーバの容量を設定し、教職員に周知しなければならない。

２　統括教育情報セキュリティ責任者は、文書サーバを学校等の単位で構成し、教職員が他の学校等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

３　統括教育情報セキュリティ責任者は、児童生徒及び教職員の個人情報、人事記録等、特定の教職員しか取り扱えないデータについて、教育情報セキュリティ管理者の協力を得て、別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、担当教職員以外の教職員が閲覧及び使用できないように設定しなければならない。

４　統括教育情報セキュリティ責任者は、インターネット接続を前提とする校務外部接続系サーバ及び学習系サーバに保管する情報（学習系サーバにおいては、機微な個人情報を保管する場合に限る。）については、標的型攻撃等によるファイルの外部流出の可能性を考慮し、ファイル暗号化等による安全管理措置を講じなければならない。

（バックアップの実施）

第43条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、次の事項に基づきバックアップを実施するものとする。

(1) 校務系情報及び校務外部接続系情報については、必要に応じて定期的にバックアップを実施しなければならない。

(2) 学習系情報については、必要に応じて定期的にバックアップを実施しなければならない。

（他団体との情報システムに関する情報等の交換）

第44条　教育情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、CISOの許可を得なければならない。

（システム管理記録及び作業の確認）

第45条　教育情報システム管理者は、所管する教育情報システムの運用において実施した作業について、作業記録を作成しなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

３　統括教育情報セキュリティ責任者、教育情報システム管理者又は教育情報システム管理者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

（情報システム仕様書等の管理）

第46条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりする等がないよう、適切に管理しなければならない。

（ログの取得等）

第47条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定期間保存しなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ログとして取得す

る項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。
3　統括教育情報セキュリティ責任者及び教育情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（障害記録）
第48条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（ネットワークの接続制御、経路制御等）
第49条　統括教育情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。
2　統括教育情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

（外部ネットワークとの接続制限等）
第50条　教育情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISOの許可を得なければならない。
2　教育情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内及び学校の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。
3　教育情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保するように努めなければならない。
4　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、教育情報ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。
5　教育情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、CISOの判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（ネットワークの分離）
第51条　教育情報システム管理者は、校務系システム及び学習系システム間の通信経路の物理的又は論理的な分離をするとともに、校務系システム及び校務外部接続系システム間の通信経路を物理的又は論理的に分離し、それぞれで適切な安全管理措置を講じなければならない。
2　教育情報システム管理者は、校務系システム、校務外部接続系システム及び学習系システム間で通信する場合には、ウイルス感染のない無害化通信など、適切な措置を図らなければならない。

（複合機のセキュリティ管理）
第52条　統括教育情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

２　統括教育情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。
３　統括教育情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（特定用途機器のセキュリティ管理）
第53条　統括教育情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（無線LAN及びネットワークの盗聴対策）
第54条　統括教育情報セキュリティ責任者は、無線LANの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。
２　統括教育情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（電子メールのセキュリティ管理）
第55条　教育情報システム管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。
２　教育情報システム管理者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。
３　教育情報システム管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。
４　教育情報システム管理者は、教職員が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を教職員に周知しなければならない。
５　教育情報システム管理者は、システム開発や運用、保守等のため施設内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

（電子メールの利用制限）
第56条　教職員は、自動転送機能を用いて、電子メールを転送してはならない。
２　教職員は、業務上必要のない送信先に電子メールを送信してはならない。
３　教職員は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
４　教職員は、重要な電子メールを誤送信した場合、教育情報セキュリティ管理者に報告しなければならない。
５　教職員は、ウェブで利用できるフリーメールサービス等を統括教育情報セキュリティ責任者の許可無しに使用してはならない。

（電子署名・暗号化）
第57条　教職員は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。
２　CISOは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（無許可ソフトウェアの導入等の禁止）
第58条　教職員は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
２　教職員は、業務上の必要がある場合は、教育情報セキュリティ管理者の許可を得て、ソフトウェアを導入することができる。
３　教職員は、不正にコピーしたソフトウェアを利用してはならない。

（機器構成の変更の制限）
第59条　教職員は、パソコンやモバイル端末に対し、機器の改造及び増設・交換を行ってはならない。
２　教職員は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括教育情報セキュリティ責任者及び教育情報システム管理者の許可を得なければならない。

（無許可でのネットワーク接続の禁止）
第60条　教職員は、統括教育情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

（業務以外の目的でのウェブ閲覧の禁止）
第61条　教職員は、業務以外の目的でウェブを閲覧してはならない。
２　統括教育情報セキュリティ責任者は、教職員のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、教育情報セキュリティ管理者に通知し適切な措置を求めなければならない。

（アクセス制御等）
第62条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員がアクセスできないように、システム上制限しなければならない。
２　利用者IDの取扱いについては、次の事項を遵守しなければならない。
(1) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、利用者の登録、変更、抹消等の情報管理、教職員の異動、出向、退職に伴う利用者IDの取扱い等の方法を定めなければならない。
(2) 教職員は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括教育情報セキュリティ責任者及び教育情報システム管理者に通知しなければならない。
(3) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、利用されていないIDが放置されないよう、人事管理部門と連携し、点検しなければならない。
３　特権を付与されたIDの管理等については、次の事項を遵守しなければならない。
(1) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理しなければならない。
(2) 統括教育情報セキュリティ責任者及び教育情報システム管理者の特権を代行する者は、統括教育情報セキュリティ責任者及び教育情報システム管理者が指名し、CISOが認めた者でなければならない。
(3) CISOは、代行者を認めた場合、速やかに統括教育情報セキュリティ責任者、教育情報セキュリティ管理者及び教育情報システム管理者に通知しなければならない。
(4) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。
(5) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたIDを初期設定以外のものに変更しなければならない。

（教職員による外部からのアクセス等の制限）

第63条　教職員が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括教育情報セキュリティ責任者及び教育情報システム管理者の許可を得なければならない。

２　統括教育情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

３　統括教育情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

４　統括教育情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

５　CISOは、公衆通信回線（公衆無線LAN等）を教育情報ネットワークに接続することは原則として禁止しなければならない。

（ログイン時の表示等）

第64条　教育情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ教職員がログインしたことを確認することができるようシステムを設定しなければならない。

（パスワードに関する情報の管理）

第65条　統括教育情報セキュリティ責任者又は教育情報システム管理者は、教職員のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

２　統括教育情報セキュリティ責任者又は教育情報システム管理者は、教職員に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

（児童生徒のID及びパスワード等の管理）

第66条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、兵庫県教育委員会（以下「教育委員会」という。）又は学校が児童生徒に個別のIDを付与する場合、利用するクラウドサービス等のID及びパスワードに対して、次の事項を含めた適切な安全管理措置を講じなければならない。

(1) IDについては唯一無二、永続的に識別可能な構成とする。パスワードについては児童生徒の発達段階に応じて複雑性を上げたものとするなど、適切な措置を講じなければならない。

(2) 卒業、退学、転出等にクラウドサービス等の利用期間が終了する場合は、あらかじめ児童生徒本人によるデータ移行を利用期間内に実施し、アカウントの利用停止後、ID及び関連するデータの削除を行わなければならない。

（情報システムの調達）

第67条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（情報システムの開発）

第68条　教育情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

２　システム開発の責任者及び作業者のIDの管理については、次の(1)及び(2)を遵守しなければならない。

(1) 教育情報システム管理者は、システム開発の責任者及び作業者が使用するIDを管理し、開発完了後、開発用IDを削除しなければならない。

(2) 教育情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

３　システム開発に用いるハードウェア及びソフトウェアの管理については、(1)及び(2)を遵守しなければならない。

(1) 教育情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

(2) 教育情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

（情報システムの導入）

第69条　開発環境と運用環境の分離及び移行手順の明確化については、次の事項を遵守しなければならない。

(1) 教育情報システム管理者は、システム開発・保守及びテスト環境とシステム運用環境を分離しなければならない。

(2) 教育情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

(3) 教育情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(4) 教育情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

２　テストについては、次の事項を遵守しなければならない。

(1) 教育情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分なテストを行わなければならない。

(2) 教育情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

(3) 教育情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

(4) 教育情報システム管理者は、開発したシステムについて受け入れテストを行う場合、 開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

(5) 教育情報システム管理者は、運用環境への移行に先立ち、システムの脆弱性テストを行い、その結果を確認しなければならない。

（システム開発・保守に関連する資料等の整備・保管）

第70条　教育情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

２　教育情報システム管理者は、テスト結果を一定期間保管しなければならない。

３　教育情報システム管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

（情報システムにおける入出力データの正確性の確保）

第71条　教育情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

２　教育情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

３　教育情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（情報システムの変更管理）

第72条　教育情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（開発・保守用のソフトウェアの更新等）

第73条　教育情報システム管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（システム更新又は統合時の検証等）

第74条　教育情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

（不正プログラム対策に関する統括教育情報セキュリティ責任者の措置事項）

第75条　統括教育情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

(1) 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

(2) 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

(3) コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ教職員に対して注意喚起しなければならない。

(4) 所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

(5) 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

(6) 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

(7) 業務で利用するソフトウェアは、教育上特別な事情があり、教育情報セキュリティ管理者が許可した場合を除き、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

（不正プログラム対策に関する教育情報システム管理者の措置事項）

第76条　教育情報システム管理者は、不正プログラム対策として、次の事項を措置しなければならない。

(1) 教育情報システム管理者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。

(2) 不正プログラム対策ソフトウェア及びパターンファイルは、常に最新の状態に保たなければならない。
(3) インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、学校が管理している電磁的記録媒体以外を教職員に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

(不正プログラム対策に関する教職員の遵守事項)
第77条　教職員は、不正プログラム対策に関し、次の事項を遵守しなければならない。
(1) パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
(2) 外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
(3) 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。
(4) 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。
(5) 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。
(6) 統括教育情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。
(7) コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。
ア　パソコン等の端末の場合
LANケーブルの即時取り外しを行わなければならない。
イ　モバイル端末の場合
直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

(専門家の支援体制)
第78条　統括教育情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

(不正アクセス対策に関する統括教育情報セキュリティ責任者の措置事項)
第79条　統括教育情報セキュリティ責任者は、不正アクセス対策として、次の事項を措置しなければならない。
(1) 使用されていないポートを閉鎖しなければならない。
(2) 不要なサービスについて、機能を削除又は停止しなければならない。
(3) 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括教育情報セキュリティ責任者及び教育情報システム管理者へ通報するよう、設定しなければならない。
(4) 統括教育情報セキュリティ責任者は、監視、通知、外部連絡窓口及び適切な対応等を実施できる体制並びに連絡網を構築しなければならない。

(攻撃の予告)
第80条　CISO及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

（不正アクセスに関する記録の保存）
第81条　CISO及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律（平成11年法律第128号）違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（内部からの攻撃）
第82条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（教職員による不正アクセス）
第83条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員による不正アクセスを発見した場合は、当該教職員が所属する学校等の教育情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

（サービス不能攻撃）
第84条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（標的型攻撃）
第85条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や事後対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

（セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等）
第86条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（不正プログラム等のセキュリティ情報の収集及び周知）
第87条　統括教育情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、教職員に周知しなければならない。

（情報セキュリティに関する情報の収集及び共有）
第88条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第８節　運用

（情報システムの監視）
第89条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティ

に関する事案を検知するため、情報システムを常時監視しなければならない。
２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

（教育情報セキュリティポリシーの遵守状況の確認及び対処）
第90条　統括教育情報セキュリティ責任者及び教育情報セキュリティ管理者は、教育情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにCISOに報告しなければならない。
２　CISOは、発生した問題について、適切かつ速やかに対処しなければならない。
３　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における教育情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

（パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査）
第91条　CISO及びCISOが指名した者は、不正アクセス、不正プログラム等の調査のために、教職員が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（教職員の報告義務）
第92条　教職員は、教育情報セキュリティポリシーに対する違反行為を発見した場合、速やかに教育情報セキュリティ管理者に報告を行わなければならない。
２　報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に報告しなければならない。
３　教育情報セキュリティ管理者は、報告のあった違反行為について、必要に応じてCISO及び教育情報セキュリティ責任者に報告しなければならない。
４　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があるとCISO及び統括教育情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

（緊急時対応計画の策定）
第93条　CISOは、情報セキュリティインシデント、教育情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

（業務継続計画との整合性確保）
第94条　自然災害、大規模又は広範囲に及ぶ疾病等に備えて、対策委員会は業務継続計画とこの対策基準との整合性を確保しなければならない。

（緊急時対応計画の見直し）
第95条　CISOは、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

（例外措置の許可）
第96条　教育情報セキュリティ管理者及び教育情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、学校事務及び教育活動の適正な遂行を継続す

るため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、CISOの許可を得て、例外措置を取ることができる。

（緊急時の例外措置）

第97条　教育情報セキュリティ管理者及び教育情報システム管理者は、学校事務及び教育活動の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにCISOに報告しなければならない。

（例外措置の申請書の管理）

第98条　CISOは、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

（法令等遵守）

第99条　教職員は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令等を遵守し、これに従わなければならない。

(1) 地方公務員法(昭和25年法律第261号)
(2) 教育公務員特例法（昭和24年法律第１号）
(3) 著作権法（昭和45年法律第48号）
(4) 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
(5) 個人情報の保護に関する法律（平成15年法律第57号）
(6) 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）
(7) 個人情報の保護に関する条例（平成８年条例第24号）

（懲戒処分等）

第100条　教育情報セキュリティポリシーに違反した教職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分等の対象とする。

（違反時の対応）

第101条　教職員の教育情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

(1) 統括教育情報セキュリティ責任者が違反を確認した場合は、統括教育情報セキュリティ責任者は当該教職員が所属する学校の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。
(2) 教育情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括教育情報セキュリティ責任者及び当該教職員が所属する学校の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。
(3) 教育情報セキュリティ管理者の指導によっても改善されない場合、統括教育情報セキュリティ責任者は、当該教職員の教育情報ネットワーク及び教育情報システムを使用する権利を停止又は剥奪することができる。その後速やかに、統括教育情報セキュリティ責任者は、教職員の権利を停止又は剥奪した旨をCISO及び当該教職員が所属する学校の教育情報セキュリティ管理者に通知しなければならない。

第９節　外部委託

（外部委託事業者の選定基準）

第102条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

（契約項目）

第103条　情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

(1) 教育情報セキュリティポリシー及び実施手順の遵守
(2) 外部委託事業者の責任者、委託内容、作業者、作業場所の特定
(3) 提供されるサービスレベルの保証
(4) 外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
(5) 外部委託事業者の従業員に対する教育の実施
(6) 提供された情報の目的外利用及び受託者以外の者への提供の禁止
(7) 業務上知り得た情報の守秘義務
(8) 再委託に関する制限事項の遵守
(9) 委託業務終了時の情報資産の返還、廃棄等
(10) 委託業務の定期報告及び緊急時報告義務
(11) 県による監査、検査
(12) 教育委員会による情報セキュリティインシデント発生時の公表
(13) 教育情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（約款による外部サービスの利用に係る規定の整備）

第104条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、次の事項を含む約款による外部サービスの利用に関する規定を整備しなければならない。

(1) サービスを利用してよい業務の範囲
(2) 利用手続及び運用手順

（約款による外部サービスの利用における対策の実施）

第105条　教職員は、利用するサービスの約款、その他提供条件から、利用にあたってのリスクが許容できることを確認した上で約款による外部サービスの利用を教育情報セキュリティ管理者に申請し、適切な措置を講じた上で利用しなければならない。

（クラウドサービスの利用）

第106条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、教育委員会又は学校が管理するアカウントでクラウドサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたクラウドサービス運用方針を定めなければならない。

(1)クラウドサービス利用者は、クラウドサービス事業者と契約時に守秘義務、目的外利用及び第三者への提供の禁止条項を締結しなければならない。
(2)クラウドサービス事業者によるクラウドサービス利用者のログの収集は、原則、クラウドサービスのシステムを起動させるための基本情報とし、学習ログ等の個人情報を目的外の利用及び第三者に提供をしてはならない。

２　重要性Ⅰの情報資産は、クラウドサービスで発信、保存してはならない。ただし、統括教育情報セキュリティ責任者及び教育情報システム管理者が認めるクラウドサービスにおいて、統括教育情報セキュリティ責任者及び教育情報システム管理者が認める重要性Ⅰの情報資産を保存する場合は、この限りではない。

３　重要性Ⅱの情報資産を、クラウドサービスで発信、保存する場合は、教育情報セキュリティ管理者の許可を得なければならない。

４　利用するクラウドサービスごとに責任者を定めなければならない。

５　クラウドサービス利用者が、卒業、退学、転出、異動、退職等により利用をしなくな

った場合には該当アカウント及びクラウド上に保存している情報資産を削除、返却しなければならない。また、削除したIDは繰り返し利用してはならない。

（ソーシャルメディアサービスの利用）

第107条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、教育委員会又は学校が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(1) 教育委員会又は学校が管理するアカウントによる情報発信が、実際の教育委員会又は学校のものであることを明らかにするために、教育委員会又は学校の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

(2) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ICカード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

２　重要性Ⅱ以上の情報資産は、ソーシャルメディアサービスで発信してはならない。

３　利用するソーシャルメディアサービスごとの責任者を定めなければならない。

第10節　評価・見直し

（監査）

第108条　CISOは、情報セキュリティ監査統括責任者を指名し、教育情報ネットワーク及び教育情報システム等の情報資産における情報セキュリティ対策状況について、毎年度監査を行わせなければならない。

（監査を行う者の要件）

第109条　情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

２　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

（監査実施計画の立案及び実施への協力）

第110条　情報セキュリティ監査統括責任者は、監査を行うにあたって、監査実施計画を立案し、対策委員会の承認を得なければならない。

２　被監査部門は、監査の実施に協力しなければならない。

（報告）

第111条　情報セキュリティ監査統括責任者は、監査結果を取りまとめ、対策委員会に報告しなければならない。

（保管）

第112条　情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

（監査結果への対応）

第113条　CISOは、監査結果を踏まえ、指摘事項を所管する教育情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない教育情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（自己点検）

第114条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、所管するネットワーク及び情報システムについて、必要に応じて自己点検を実施しなければならない。

２　統括教育情報セキュリティ責任者は、教育情報セキュリティ管理者と連携して、所管する学校等における教育情報セキュリティポリシーに沿った情報セキュリティ対策状況について、必要に応じて自己点検を行わなければならない。

（報告）

第115条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、対策委員会に報告しなければならない。

（自己点検結果の活用）

第116条　教職員は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

２　対策委員会は、自己点検結果をこの対策基準及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（対策基準及び関係規程等の見直し）

第117条　対策委員会は、監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、この対策基準及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

附　則

１　この対策基準は、令和２年９月１日から施行する。

２　兵庫県教育情報ネットワーク運営管理要綱（平成11年４月１日制定）は、廃止する。

３　この対策基準は、令和４年４月１日から施行する。

４　この対策基準は、令和５年４月１日から施行する。

５　この対策基準は、令和６年４月１日から施行する。