# INVITATION FOR BID (IFB) TEMPLATE

## Instructions for Using the IFB Template

* This IFB template has been completely revised to accommodate the new business processes initiated as a result of implementing the State Procurement Bureau’s electronic procurement system, eMACS. The sections that were defined in the old paper IFB process have been removed. All that is left are the particular clauses that require decisions to be made by the agency.
* Instructions to agencies appear in **blue**.
* Insert appropriate information when requested in areas that appear in **red**.
* Decide which optional paragraphs are needed and delete those not needed.
* If you are preparing an IT IFB, be sure to include all language specific to IT projects.
* If appropriate, include a copy of the contract you intend to use.
* For all solicitations for which Prevailing Wage Rates will be paid, the applicable Prevailing Wage Booklet from the Department of Labor and Industry must be included as part of the solicitation. Current Prevailing Wage Booklets are available [Department of Labor and Industry Website](http://erd.dli.mt.gov/labor-standards/state-prevailing-wage-rates).
* Call the State Procurement Bureau with questions at 406-444-2575.

**Tips for fillable WORD documents:**

1. When you click on the text and see Click to Delete, you can select the word or sentence to delete.



1. You will also have the option to click on the text and enter the appropriate information.



GENERAL REQUIREMENTS

#### CONTRACT TERM

The contract term is for a period of enter number years beginning enter start date and ending enter end date. Renewals of the contract, by mutual agreement of both parties, may be made at enter number-year intervals, or any interval that is advantageous to the State. This contract, including any renewals, may not exceed a total of enter number years, at the option of the State.

NOTE TO AGENCIES: State contracts generally may not exceed a total of seven years, IT contracts for 10 years.

#### PRE-BID CONFERENCE

**An optional/A mandatory** Pre-Bid Conference will be conducted at enter location on enter date at enter time. Bidders are encouraged to use this opportunity to ask clarifying questions, obtain a better understanding of the project, or to notify the State of any ambiguities, inconsistencies, or errors discovered upon examination of this IFB. All responses to questions at the Pre-Bid Conference will be oral and in no way binding on the State.

OR

**An optional/A mandatory** Pre-Bid Telephone Conference Call will be conducted on enter date at enter phone number at enter time. Bidders are encouraged to use this opportunity to ask clarifying questions, obtain a better understanding of the project, or to notify the State of any ambiguities, inconsistencies, or errors discovered upon examination of this IFB. All responses to questions at the Pre-Bid Conference will be oral and in no way binding on the State. Participation in the conference call is optional. However, it is advisable that all interested parties participate. To participate, call (406) enter phone number. The password is enter password.

Descriptive Literature

Complete manufacturer’s descriptive literature sufficient in detail to establish quality and compliance with all specifications must be submitted with each bid. The State reserves the right to examine products further to determine compliance with the stated specifications.

### DELIVERY REQUIREMENTS

Delivery Date

The DELIVERY DATE in Items must be completed to indicate day, month, and year, or a specific number of days after receipt of order (ARO). Failure to comply with the requirements may invalidate a bidder’s quotation for any or all items.

Requested Delivery Date

The Contractor shall deliver all items described in this bid as soon as possible but no later than enter date after receipt of purchase order from the State of Montana.

#### OR

Guaranteed Delivery

Due to the immediate need of the user agency, delivery must be guaranteed to be completed on or before enter date.

Shipping

Weekends and holidays excepted, deliveries shall be **F.O.B. DESTINATION**, to the location shown below. The term "F.O.B. destination, within the State's premises," as used in this clause, means free of expense to the State and delivered to the location specified. The Contractor shall:

* Pack and mark the shipment to comply with specifications; or if the specifications do not contain specific packing or marking instructions, pack and mark the shipment in accordance with prevailing commercial practices and in such a manner as to ensure delivery in good condition and as required by this IFB;
* Prepare and distribute commercial bills of lading and Material Safety Data Sheets (MSDS) as appropriate;
* Deliver the shipment in good order and condition to the point of delivery specified in the IFB;
* Be responsible for any loss of and/or damage to the goods occurring before receipt of the shipment by the State at the delivery point specified in the IFB;
* Furnish a delivery schedule and designate the mode of delivering carrier; and
* Pay and bear all charges to the specified points of delivery.

#### Delivery Locations

Insert Delivery Locations

**Be specific about the location, include physical address, room numbers, etc.)**

### SPECIAL TERMS AND CONDITIONS

This section must be tailored to each project. Call SPB for assistance at 406-444-2575.

All items listed in this section are optional. If a contract or PO is attached to the IFB most of the following clauses will be found there and should be deleted from this section.

#### PREFERENCE NOT APPLIED

Reciprocal preference will not be applied to this purchase because federal funds are involved (ARM 2.5.408).

#### PURCHASING CARD

The State of Montana has a Purchasing Card Program in place that gives agencies the ability to charge purchases made from these contracts. The State of Montana prefers this method of payment.

#### ON-SITE REQUIREMENTS/CLEANUP

Each potential contractor should visit the job site to verify measurements and to become fully aware of the conditions relating to the project and the labor requirements. Failure to do so will not relieve the successful contractor of their obligation to furnish all materials and labor necessary to carry out the provisions of the contract.

The Contractor shall adequately protect the work, adjacent property, and the public in all phases of the work. The Contractor shall be responsible for all damages or injury due to their action or neglect.

The Contractor shall maintain access to all phases of the project pending inspection by the State or its representative.

All work rejected as unsatisfactory shall be corrected prior to final inspection and acceptance.

The Contractor shall respond within seven calendar days after notice of observed defects has been given and shall proceed to immediately remedy these defects. Should the Contractor fail to respond to the notice or not remedy the defects, the State may have the work corrected at the Contractor's expense.

*(Insert applicable provisions)*

In terms of cleanup, the Contractor shall:

(a) Keep the premises free from debris and accumulation of waste;

(b) Clean up any oil or fuel spills;

(c) Keep machinery clean and free of weeds;

(d) Remove all construction smears and stains from finished surfaces;

(e) Perform finishing site preparation to limit the spread of noxious weeds before final payment by the State; and

(f) Remove all construction equipment, tools, and excess materials before final payment by the State.

#### REQUIRED INSURANCE

*(Insert for commercial general liability and automobile liability only)*

General Requirements

The Contractor shall maintain for the duration of the contract, at its cost and expense, insurance against claims for injuries to persons or damages to property, including contractual liability, which may arise from or in connection with the performance of the work by the Contractor, agents, employees, representatives, assigns, or subcontractors. This insurance shall cover such claims as may be caused by any negligent act or omission.

*(Insert for all insurance types)*

Primary Insurance

The Contractor's insurance coverage shall be primary insurance with respect to the State, its officers, officials, employees, and volunteers and shall apply separately to each project or location. Any insurance or self-insurance maintained by the State, its officers, officials, employees or volunteers shall be excess of the Contractor's insurance and shall not contribute with it.

*(Insert for commercial general liability only)*

Specific Requirements for Commercial General Liability

The Contractor shall purchase and maintain occurrence coverage with combined single limits for bodily injury, personal injury, and property damage of insert dollar amount per occurrence and insert dollar amount aggregate per year to cover such claims as may be caused by any act, omission, or negligence of the Contractor or its officers, agents, representatives, assigns, or subcontractors.

The State, its officers, officials, employees, and volunteers are to be covered and listed as additional insureds; for liability arising out of activities performed by or on behalf of the Contractor, including the insured's general supervision of the Contractor; products, and completed operations; premises owned, leased, occupied, or used.

*(Insert for automobile liability only)*

Specific Requirements for Automobile Liability

The Contractor shall purchase and maintain coverage with split limits of $500,000 per person (personal injury), $1,000,000 per accident occurrence (personal injury), and $100,000 per accident occurrence (property damage), OR combined single limits of $1,000,000 per occurrence to cover such claims as may be caused by any act, omission, or negligence of the contractor or its officers, agents, representatives, assigns, or subcontractors.

The State, its officers, officials, employees, and volunteers are to be covered and listed as additional insureds for automobiles leased, hired, or borrowed by the Contractor.

*(Insert for professional liability only)*

Specific Requirements for Professional Liability

The Contractor shall purchase and maintain occurrence coverage with combined single limits for each wrongful act of insert dollar amount per occurrence and insert dollar amount aggregate per year to cover such claims as may be caused by any act, omission, negligence of the Contractor or its officers, agents, representatives, assigns, or subcontractors. Note: if "occurrence" coverage is unavailable or cost prohibitive, the Contractor may provide "claims made" coverage provided the following conditions are met: (1) the commencement date of the contract must not fall outside the effective date of insurance coverage and it will be the retroactive date for insurance coverage in future years; and (2) the claims made policy must have a three-year tail for claims that are made (filed) after the cancellation or expiration date of the policy.

*(Insert for all insurance types)*

Deductibles and Self-Insured Retentions

Any deductible or self-insured retention must be declared to and approved by the state agency. At the request of the agency either: (1) the insurer shall reduce or eliminate such deductibles or self-insured retentions as respects the State, its officers, officials, employees, or volunteers; or (2) at the expense of the Contractor, the Contractor shall procure a bond guaranteeing payment of losses and related investigations, claims administration, and defense expenses.

*(Insert for all insurance types)*

Certificate of Insurance/Endorsements

A certificate of insurance from an insurer with a Best's rating of no less than A- indicating compliance with the required coverages, has been received by the State Procurement Bureau, P.O. Box 200135, Helena, MT 59620-0135. The Contractor must notify the State immediately, of any material change in insurance coverage, such as changes in limits, coverages, change in status of policy, etc. The State reserves the right to require complete copies of insurance policies at all times.

### SPECIFICATIONS AND PRICING

This section needs to be tailored to each project. Call SPB for assistance at 406-444-2575.

#### EQUIVALENT PRODUCTS

Requirements designated in this bid must be satisfied, or a functional equivalent bid submitted, which is acceptable to the State. Bidders who do not meet this criterion may be disqualified from further consideration. A bidder must state if they are unable or unwilling to meet any requirement. Inability or unwillingness to meet any requirement, in part or total, may be cause for disqualification of the entire response. Any exceptions taken by the bidder must be clearly identified on the bid forms.

OR

#### SPECIFIC BRAND

The following specifications identify specific brand requirements of this Invitation for Bid. Only quotations for the brand specified will be considered for award.

Sole Brand requests must be submitted to State Procurement for approval prior to release of the solicitation.

#### PRICES

##### **Fixed Price Contract**

All prices are fixed for the duration of the contract and are not subject to escalation for any cause. Payment of the total fixed bid price shall constitute full payment for performance of the work and covers all costs of whatever nature incurred by the Contractor in accomplishing the work in accordance with the provisions of the contract.

OR

##### **Cost Increase by Mutual Agreement**

After the initial term of the contract, each renewal term may be subject to a cost increase by mutual agreement.

OR

##### **Cost Increase by Fixed Amount**

After the initial term of the contract, each renewal term may be subject to a cost increase of insert number%, not to exceed insert number%, for the entire term of the contract.

OR

##### **Pricing Adjustments per Increase in CPI**

Annual pricing adjustments to contract renewals following the contract term, if applicable, shall not exceed 75% the rate of increase in the cost of living as reflected in the Federal Bureau of Labor Statistics, Consumer Price Index (CPI) for all Urban Consumers (1982-84 = 100; through November 1991 = 137.8) or any other index which may be substituted in the future. The CPI for the last 12-month period of the contract will be the CPI base on which later adjustments are computed. Each time an adjustment is made, the earlier CPI base will be replaced by the adjusted CPI base. The percentage of adjustment to contract prices shall in no event exceed the percentage change in the index.

OR

##### **Price Adjustments Negotiated Based on Changes in Contractor's Costs**

Price adjustments may be permitted at the time of contract renewal through a process of negotiation with the Contractor and the State. Any price increases must be based on demonstrated industrywide or regional increases in the Contractor's costs. Publications such as the Federal Bureau of Labor Statistics and the Consumer Price Index (CPI) for all Urban Consumers may be used to determine the increased value.

##### ITEM-BY-ITEM OR ALL-OR-NONE AWARD

Awards will be made on an **(Item-by-item OR all-or-none)** basis. Failure of a bidder to provide prices for all line items listed on the Schedule may be cause for rejection of the entire bid. However, a bidder may enter "No Cost" in the unit price and extended amount columns to indicate that the item is being offered at "No Cost."

#### SPECIFICATIONS

Insert item specifications. Tailor as appropriate.

Specifications provide a precise description of the critical features a supply or service must have to satisfy an agency's needs. A specification should be written from the general to the specific. The following outline may be used as a guideline:

###### **Name of Supply or Service:** Begin a specification by listing the name of the supply or service sought: "compact sedan," for example, or "photocopier maintenance." Do not list a specific brand name in the title.

###### **Purpose/Use for Supply or Service:** State the purpose for which the item will be used. For example, a lawn mower specification might be: "suitable for daily use (4-6 hours) on a large grounds complex." Vendors should know the intended use to decide what type of product to bid.

###### **Description of Supply or Service:** List all the critical features the product must perform or have to meet agency requirements. Use a specification that indicates **performance** requirements if the agency is interested in the end product. Use a **design** specification, which details how a product is engineered, if the agency is interested in how a product will achieve that end result, or if the agency has a specific physical requirement for the product. Agencies should recognize that it is difficult to draft design specifications without being restrictive and limiting competition. A combination of performance and design requirements is often the most ideal specification.

Identify the minimum requirements, but make sure the stated minimum is a product that will satisfy the agency. If there are **brand-name-or-equal** products that are of the appropriate quality level, list several of the brand names and model numbers, indicating the level or quality desired. However, this does not indicate a restriction to or acceptance of only those brands.

Agencies need to be careful to not imply that only a certain brand name would be acceptable when preparing their bid specifications. Agencies should conduct product research to locate additional brands that may be able to meet their needs.

If a single brand name is necessary to provide the necessary quality, written justification must be provided using the State Procurement Bureau's "Sole Brand" Justification Form located at [SPB’s Website](https://spb.mt.gov/Procurement-Guide) (ARM 2.5.501).

###### **List Special Requirements:** Provide any special requirements that the product or vendor must perform. Warranty, service, parts, and training requirements must be listed.

###### **Unusual Conditions:** Describe any unusual conditions, such as installation, field test, fiscal year funding source, etc.

###### **Receiving Procedures:** Describe if necessary, any receiving procedures (if testing, sampling, or other evaluation will be performed when commodity is delivered to determine acceptability).

### SECURITY AND PRIVACY CONTROL REQUIREMENTS

Through policy, the State of Montana’s Chief Information Officer (CIO) has determined that the State of Montana shall follow the National Institute of Standards and Technology (NIST) security guidelines and the Federal Information Security Management Act (FISMA). Any personally identifiable information from the system that is used by or available to the contractor, its employees, its subcontractors, and the employees of its subcontractors must be kept confidential and data shall only be shared in accordance with applicable interconnection security agreements, business associate agreements, computer matching agreements, and/or privacy protection agreements. The Contractor must comply with all requirements, as provided in the current revision of the [NIST SP 800-53](https://nvd.nist.gov/800-53), for a moderate impact system, and must provide annual assurance of such compliance.

#### The Contractor shall meet each of the security and system integrity requirements as referenced below:

##### The Bidder shall provide a description of relevant experience relating to the services/products requested in this IFB.

NOTE TO AGENCY: If this IFB is for Software OR Hardware please REMOVE Section 2 and 2.1-2.14. If this IFB is for Software as a Service (SaaS) or a Major Application INCLUDE Section 2 and 2.1-2.14

##### The Contractor shall create and maintain a formal system security plan that complies with all NIST SP 800-53 security requirements relating to a moderate impact system that, at a minimum:

* 1. Is consistent with the State of Montana’s [enterprise architecture](https://sitsd.mt.gov/Services-Support/Enterprise-Architecture);
  2. Explicitly defines the authorization boundary for the system;
  3. Describes the operational context of the information system in terms of mission and business processes;
  4. Provides the security categorization of the information system, as established by the State, including supporting rationale;
  5. Describes the operational environment for the informational system and relationships with or connection to other information systems;
  6. Provides an overview of the security requirements for the system;
  7. Identifies any relevant overlays, if applicable;
  8. Identifies any specific statutory and/or regulatory requirements (above and beyond the requirements stated in the current version of the NIST SP 800-53 Moderate Baseline Controls), if applicable;
  9. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions;
  10. Is accepted by the authorizing official or designated representative prior to plan implementation;
  11. Is distributed to appropriate personnel;
  12. Is reviewed and updated, at least annually, or whenever changes to the information system/environment of operation occur; and
  13. Is protected from unauthorized disclosure and modification.
  14. Describes in detail the process and plans to update the application to stay current with platforms and infrastructure.

##### The Contractor shall provide identification and authentication requirements for the system and provide integration with State of Montana network technologies. If the proposed system is to be hosted outside of the state network, access control can be used throughOKTA.

##### The Contractor shall provide the process used to notify customers of application downtime for both planned and unplanned outages.

##### The Contractor shall describe in detail if the proposed system utilizes remote access for management of the system. Awardee must describe plans to use enterprise approved mechanisms for remote access.

##### The Contractor’s proposed solution shall support Federal Information Processing Standards (FIPS) 140-2 compliant encryption.

Note to agency: If this IFB is for Software OR Hardware please REMOVE Section 7 and 7.1-7.2 If this IFB is for Software as a Service (SaaS) or a Major Application INCLUDE Section 7 and 7.1-7.2

##### The Contractor shall provide in detail a security incident response plan.

* 1. The Contractor must report security incidents that occur on the [agency] information systems that may affect [agency] or the State of Montana systems to the [agency] Chief Information Officer OR the designee as directed by the [agency] within 24 hours of discovery.
  2. The Contractor must provide, in detail, incident reporting processes and how an incident will be communicated to customers during an incident.

Note to agency: If this IFB is for Software OR Hardware please REMOVE Section 8 If this IFB is for Software as a Service (SaaS) or a Major Application INCLUDE Section 8

##### The Contractor shall provide, in detail, a disaster recovery plan addressing the intended recovery efforts for the proposed system and data.

Note to agency: If this IFB is for Software please REMOVE Section 9 If this IFB is for Software as a Service (SaaS) or a Major Application INCLUDE Section 9

##### The Contractor shall describe, in detail, auditable events to be employed that would support after-the-fact investigations of security incidents, ensure that audit logs are retained for seven years and be made available upon request to the State or investigators. Audit logs must establish the type of event that occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

1. The Contractor shall provide for inspections, by State personnel, State designee, or regulatory bodies and provide access to information and the environment, upon receiving a reasonable request from the State.
2. The Contractor shall provide annual security awareness and applicable role-based training to all concerned staff members.

11.1 The Contractor shall provide the Contract Liaison with a description and proof of completion of the security training given to the Contractor’s staff that have direct or indirect access to the proposed system.

1. The Contractor shall provide an overview of security practices of the Contractor regarding secure application development.
2. The Contractor shall provide administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

##### The Contractor shall provide user documentation for the information system, system component, or information system service that describes:

* 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
  2. Methods for user interaction, which enable~~s~~ individuals to use the system, component, or service in a more secure manner; and
  3. User responsibilities in maintaining the security of the system, component, or service.

The Contractor shall provide documentation on how the proposed system can or cannot meet each of the **Privacy** requirements, as referenced below.

##### The system shall provide and the Contractor must document privacy protections that include:

Statements of purpose for the collection of personally identifiable information;

Data quality and integrity checks that provide for validation and verification of personally identifiable information;

Data minimization and retention checks that ensure personally identifiable information collected, used, and retained is relevant and necessary for the purpose for which it was originally collected.

Information about location of data storage, addressing requirements to keep all data in the United States.

Data collected by proposed system will remain under the ownership of State of Montana, and will be made available on request by [agency] or termination of contract.

The Contractor will not copy any State data obtained while performing services under this IFB to any media, including hard drives, flash drives, or other electronic devices, other than as expressly approved by [agency].

The Contractor shall return all data that is the property of the State of Montana in a format specified by the State.

The Contractor shall return all data to the State of Montana upon completion or termination of the contract.

The Contractor shall return all sensitive information received from the State or created/received by Contractor on behalf of the State in a manner that is documented and consistent with the State’s policy on sanitization of information system media (both digital and non-digital), with sanitization mechanisms that are commensurate with the classification or sensitivity of that information.

If the State agrees that return or destruction of confidential information is infeasible; Contractor shall extend the protections of this IFB and or subsequent contract to such confidential information and limit further uses and disclosures of such confidential information to those purposes that make the return or destruction infeasible, for so long as Contractor maintains such confidential information.

##### The Contractor shall provide notice of a loss or suspected loss of privacy data to the [agency] Chief Information Officer, or designee as directed by the agency, within 24 hours of loss or suspected loss.

## Physical Security Language

Please use the following criteria in determining escorted versus unescorted Access:

There are three levels of access to the data centers – controlling access, escorted access and unescorted access.

Controlling access is given to employees who have unlimited access authority to the data centers.

1. Controlling Access is given to employees who have unlimited access authority to the Data Centers.
   1. Controlling Access is granted to the staff whose job responsibilities require that they have access to the area on a day-to-day basis. These individuals also have the authority to grant temporary access to a Data Center and to enable others to enter and leave a Data Center. People with Controlling Access are responsible for the security of the area, and for any individuals that they allow into a Data Center. Individuals with Controlling Access to a Data Center normally will be granted access via a cardkey and will be placed on the Data Center Access List. These individuals must wear their State Identification Card visibly at all times while in a Data Center. Any individual receiving Controlling Access must go through a formal background check according to their identified risk designation (see the Personnel Security Policy, Personnel Security Procedure, and Background Checks for Contractors, Lessees, and External Personnel Procedure).
   2. Individuals granted controlling access may, in addition to the cardkey they are issued, request key access. While it is not a best practice to issue keys to a Data Center for routine access purposes, requests for this type of access will be considered on a case-by-case basis.
   3. In addition to cardkey access, individuals granted controlling access will be required to gain physical access using two-factor authentication. Two-factor authentication uses biometrics in addition to the cardkey to provide access to some secured areas.
   4. Individuals with Controlling Access to an area may allow authorized and logged individuals Escorted or Unescorted Access to a Data Center.
   5. If a person with Controlling Access allows Escorted Access to an individual, the person granting access is responsible for escorting the individual granted access and seeing to it that they sign in and out on the access log. If needed, these duties can be handed-off to one of the staff that is on duty in a Data Center.
2. Escorted Access is closely monitored access given to people who have a legitimate business need for infrequent access to a Data Center. “Infrequent access” is generally defined as access required for less than 15 days per year.
   1. Individuals with Escorted Access will not be issued keys or be granted access via cardkey.
   2. A person given Escorted Access to an area must sign in and out on the access log under the direct supervision of a person with Controlling Access or Unescorted Access. They must also provide positive identification upon demand and must leave the area when requested to do so.
   3. A person given escorted access will be given a “Visitor” badge after they sign in, which must be worn visibly at all times.
   4. A person with Escorted Access to an area must not allow any other person to enter or leave the area.
3. Unescorted Access is granted to a person who does not qualify for Controlling Access but has a legitimate business reason for unsupervised access to a Data Center. An example of this would be a State Employee or Approved Vendor who requires access to work on their system for a set period of time.
   1. Individuals with Unescorted Access to a Data Center will be granted access to the area via cardkey. For additional process information regarding individuals with unescorted access, see the Temporary Badge Procedure.
   2. Persons with Unescorted Access should only enter a Data Center to perform tasks that cannot be performed remotely.
   3. Unescorted Access personnel cannot authorize others to be granted access to a Data Center. They must alert someone with Controlling Access that they will be escorting a Staff Employee or Approved Vendor that themselves do not have Data Center access.
   4. All individuals with Unescorted Access must wear their badge visibly at all times while in a Data Center.

**Data Center Doors**

1. All doors to a Data Center must remain locked at all times and may only be temporarily opened for periods not to exceed that minimally necessary in order to:
2. Allow officially approved and logged entrance and exit of authorized individuals.
3. Permit the transfer of supplies/equipment as directly supervised by a person with Controlling Access to the area. Internal and external doors will not be allowed to be opened at the same time except for cases where increased airflow is required (see item #3 below).
4. Doors to the Data Center will ONLY be propped open if it is necessary to increase airflow into the Data Center in the case of an air conditioning failure. In this case, staff personnel with Controlling Access must be present to limit and monitor access to the Data Center.

**Security System and Keys**

1. Keys to a data center are not generally issued for routine access purposes. The following information pertains to keys and the security system:
2. If a key is provided, the individual receiving the key may not share, loan or copy it.
3. Only those people who have been granted Controlling Access can request and be issued keys.
4. Under no circumstances may an individual attempt to bypass the cardkey system to gain access for them or permit access to another individual by using a key.
5. Individuals are not to share their cardkey.
6. If the biometric system being used fails, employees will be allowed into the facility by an employee with controlling access who can identify them. The accessing employee must show their cardkey to the employee with controlling access before entry into the secured facility will be allowed.

**Review and Removal of Access**

1. Monthly reviews will be performed of physical access to the Data Centers. If an individual no longer requires access to a Data Center or if the cardkey has been inactive for more than 90 days, the access will be removed.
   1. For Individuals whose access is removed for termination or no business need:
      1. In the Data Center Access List, they will be reclassified as “De-active”
      2. In the Bio-Metric system their fingerprint will be deleted
   2. For individuals whose access is removed because of inactivity for more than 90 days and they do not have a 90-day exception:

Notification will be sent to the individual whose access has been removed for inactivity for more than 90 days.

* + 1. In the Data Center Access list, they will be reclassified as Access – Inactive 90 days
    2. In the Bio-Metric system their fingerprint will be disabled.
    3. They can access the Data Center if their Authorization Granted in the Data Center Access List is less than three years old and no one has revoked their access. They will be issued an active visitor badge to perform their duties.
  1. [90-Day] Exception Process:
     1. Any individual with cardkey and bio-metric access can ask to be part of the 90-Day exception group. Examples would be State Employees or Authorized Vendors needed for emergency response, Authorized Vendors that are contractually obligated to respond in a given time frame that may require access during unoccupied times of a Data Center.
     2. Requests must be submitted by a person’s supervisor if a State Employee or by the supervisor in charge of an Authorized Vendors contract.
     3. The request must be given to the ISB office for review by the CISO.

1. Periodic (at least annual) reviews will be performed on the location of keys to the Data Centers. If an individual no longer needs a key, it will be collected.
2. Procedures for removing access to a Data Center include:
   1. Canceling cardkey access
   2. Collecting a key
   3. Removing the person’s name from the Data Center Access List
3. The results of periodic reviews will be reported to the SITSD Information Systems Security Officer. The report will include an updated list of those allowed access to the Data Centers.

**Data Center Access List**

1. The Data Center Access List is managed by Data Center Facilities staff.
2. Individuals with Controlling Access to a Data Center (not just Data Center staff) are responsible for maintaining the Data Center Access List. The following procedures must be followed:
   1. Each time an individual with Escorted Access to a Data Center is admitted to an area, he/she must properly sign in on the Data Center Access List at the time of entrance.
   2. The person admitting the visitor must countersign and fill out the appropriate section of the form. The visitor must also present a picture identification card for verification of identity.
   3. Each time an individual with Escorted Access leaves the area, he/she must properly sign out on the Data Center Access List at the time of exit. NOTE: If an individual will be coming and going throughout the day, they can sign in and out one time for that day.
   4. The person escorting the visitor when they leave must fill out the “Time Out” section of the Sign in Sheet.

**Incident Reporting**

1. All infractions of the Data Center Physical Security Policies and Procedures shall be reported to the ISB. If warranted (e.g.: emergency, imminent danger, etc.) law enforcement should be notified as soon as is reasonably possible.
2. All high-profile incidents will be reported to the SMDC Lead/Manager on site, the Manager-on-call, or the ISB immediately. Examples of high-profile incidents are: an unauthorized individual in the Data Center, any attempt to enter a Data Center forcibly or improperly, missing or damaged equipment, etc.
3. Individuals with Controlling Access to the area are to monitor the area and have individual who appears to be compromising either the security of the area or its activities, or who is disrupting operations, removed. The State reserves the right to remove any contractor personnel who appear to be compromising the security. It is particularly important that individuals with Controlling Access show initiative in monitoring and maintaining the security of the Data Center.

**Requesting Access to the Data Centers**

1. All physical access to the Data Centers is granted according to group policy. Each person will be granted access according to the group for which they are associated.
2. **Contractors:**

2.1 Contract Administrators can request physical access for contractors to a data center. For process information on physical access and background checks for contractors, see the Physical Access Controls Procedure, and the Background Checks for Contractors, Lessees, and External Agency Personnel Procedure.

**Emergency Access**

If it becomes necessary to provide emergency access to medical, fire, and/or police officials, the escorted access procedure can be temporarily suspended.

**Other Information**

No camera or photographic equipment will be allowed within the Data Center without the approval of the SMDC Manager or ISB.