

February 9, 2026

Ms. Shannon Simmers
Interim Environmental Services Coordinator
City of Riverside
5950 Acorn Street
Riverside, CA 92504

Subject: Proposal: iPACS System Maintenance Services (Two Years for FY27 & FY28), Revision 2

Dear Shannon:

The City of Riverside uses enfoTech iPACS system to manage pretreatment programs compliance data mandated under the USEPA 40CFR regulations. enfoTech provides iPACS v.6 to City under a software-as-a-service agreement and will provide services. City's current iPACS service Agreement will expire on 6/30/2026. enfoTech presents this proposal to expand the current Agreement for two more years.

(1) Work Scope and Cost

enfoTech will provide the following services.

ID	Service Period	Services	Cost	Payment Due
1	From 7/1/2026 to 6/30/2027	iPACS SaaS software Hosting & Technical Support (see Attachment A for details)	\$ 36,120	6/30/2026
2	From 7/1/2027 to 6/30/2028	iPACS SaaS software Hosting & Technical Support (see Attachment A for details)	\$ 37,926	6/30/2027
3	From 7/1/2026 to 6/30/2027	iPACS system enhancements	See section 2 below	Based on deliverable

(2) System Enhancement Services

Upon City's request, enfoTech will provide technical services to enhance iPACS to address regulatory changes and process improvements. For budget planning purpose, enfoTech provides a budget estimate for the following items.

Enhancement Description	Cost Range	
	Lower	Upper
1. Change existing Permit templates (Class 1, Class 2, Liquid waste, O/G)	\$5,760	\$7,200
2. Update one inspection form (plus 1 SSRS report for inspection report)	\$2,560	\$3,200
3. Update one existing SSRS report	\$2,720	\$3,400
4. Create one new SSRS report	\$4,160	\$5,200
5. Create one new inspection form (plus 1 SSRS report for inspection report)	\$6,080	\$7,600
	\$21,280	\$26,600

Actual spending will be based on system enhancement scope, respective labor rates, and expenses. For each service request, City will provide requirements to enfoTech and requests a work order. enfoTech will provide a work order based on specifications, estimated delivery schedule, and cost. City will comment and approve the work order and, after mutual discussions, provide an approval for enfoTech to engage the work. City has the discretion to reallocate enhancement funding to other services or carry unused funding to subsequent years.

(3) Labor Rates for Additional Services

Professional Labor Category	Hourly Rate (\$)		Professional Labor Category	Hourly Rate (\$)
1. Principal Consultant	\$250		2. Database Administrator	\$185
3. Project Manager	\$220		4. Database Administrator (DBA)	\$185
5. Solution Architect	\$210		6. Business Analyst	\$180
7. System Developer	\$185		8. QA/QC Specialist	\$165

(4) Payment Schedule

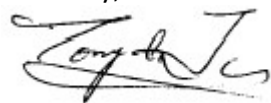
- iPACS Annual Hosting & Technical Support fee will be payable prior to the begin date of each service period
- System enhancements fees will be invoiced based on time spent, respective labor rate, expenses.
- enfoTech will submit invoices to the City for deliverables completed under the purchase order.
- enfoTech payment terms are 30 days net from the invoice date.

(5) Sole Source Justification

iPACS and associated systems are developed by enfoTech. enfoTech owns the product’s Titles and is the only entity that is authorized to license the software systems and to provide technical services. We do not have any local distributor or service agent for the sale or support of the software.

This proposal is valid for 120 days from the date of submission. Thank you for the opportunity to present this proposal to the City for evaluation. Please contact us for any questions or clarifications. We look forward to continue serving the City of Riverside.

Sincerely,



Tony C. Jeng
 Executive Vice President

Enclosures

cc: File – City of Riverside, Sony Su

Attachment A: iPACS System Hosting & Support Services

(A) Hosting Services

enfoTech maintains three system hosting locations all within the USA.

1. **Primary Site:** the primary hosting location is a colocation at Iron Mountain Data Center located at 3003 Woodbridge Ave, Edison, NJ 08837 (<https://datacenter.ironmountain.com>) enfoTech co-location the Data Center and owns 100% of equipment and software for our SaaS services. The center has 100% uptime performance record since 2006. The Data center is SSAE-16 and HIPAA certified.

Primary Managed Share Servers

- Primary Data Center & Hosting Site:
 - Facility: Data Center Managed Network Services
 - URL: <https://datacenter.ironmountain.com>
- Capacity
 - Internet bandwidth: 1000 mbps
 - Server Internal Network Speed: 1000 Mbps or up
 - Server security protection (HTTPs certification through GoDaddy)
 - External Storage Connection(s): Private Backup Network Connection
 - Standard Drive Partitioning: C: and E: - dual partitions
 - Microsoft Web/ASP.NET Best Practices Installation
 - Automated Monitoring Alerts with system down notification (to enfoTech system staff)
 - Managed Anti-Virus



2. **Secondary Site:** is located at Iron Mountain Data Center. The Secondary site:
 - a. Has a completely different set of redundant services equivalent to the Primary site.
 - b. There is a High-Availability hardware and software redundancy between the Primary and Secondary sites.
 - c. Both the Systems and the Databases are replicated from the Primary to the Secondary.

If the Primary site becomes non-functional, the Secondary site will be automatically switched on to provide services.

3. **Tertiary Site:** is located at enfoTech headquarters at 1368 How Lane, North Brunswick, NJ 08902 (<http://www.enfotech.com>) There is a minute-by-minute backup service of the systems and databases from the Secondary site to the Tertiary site. If both the Primary and Secondary sites become non-functional, the Tertiary site will be automatically brought to services within 8-24 hours.

- Capacity:
 - Internet bandwidth: 1,000 Mbps
 - Server Internal Network Speed: 10,000 Mbps or up
 - Server security protection (HTTPs certification through GoDaddy)
 - External Storage Connection(s): Private Backup Network Connection
 - Standard Drive Partitioning: C: and E: - dual partitions
 - Microsoft Web/ASP.NET Best Practices Installation
 - Automated Monitoring Alerts with system down notification (to enfoTech system staff)
 - Managed Anti-Virus

4. Tertiary DR Replication Site

Security Measure	Description
1. Firewall	▪ Physically different location. Equivalent hardware to the Primary site.
2. DMZ Zone Servers	▪ Physically different location.
3. Load Balancers	▪ Physically different location. Different hardware with capability equivalent to the Primary site.
4. LAN Servers	▪ Physically different location. Different hardware with capability equivalent to the Primary site.
5. Application	▪ Physically different location. Replicated from Primary site.
6. Database	▪ Physically different location. Replicated from Primary site.
7. Data Vault	▪ Complete replication of Systems which includes OS, application, configurations, and database
8. IDP (Intrusion, Detection, Prevention)	▪ Monitoring all entry attempts, detect potential risks, prevent potential attacks, issue alerts ▪ Enhanced Identity Management
9. Replication from the Primary Hosting Site to the DR Replication Site	▪ Replication will continue with 15 minutes lag ▪ The Tertiary site will be brought to services within 8-24 hour after both the primary and secondary sites are down

5. Quaternary Remote Backup Site (Off-site)

Security Measure	Description
1. Data Vault	▪ Complete replication of SYSTEM which includes OS, application, configurations, and database
2. Replication from the Tertiary DR replication site	▪ Offline replication. Replication will be synchronized with the Tertiary DR Replication servers. ▪ The Backup site will be brought to services within 2 to 3 days after all sites are down

6. Data Center Classification

- **Network / Internet Service Provider Classification:**
 There are **three** Network/ISP Tiers (1, 2, and 3), with Tier 1 being the highest level. enfoTech is tier 2 ISP, which purchases Internet service from a tier 1 ISP such as Verizon, AT&T, and Level 3 Communications etc.

- **Cloud Infrastructure Classification:**

There are **four** tiers of cloud infrastructure, with Tier 4 being the highest level in this classification. enfoTech is a tier 3+ provider as it includes more than one distribution path for data. This makes the IT equipment within the organization run smoother because information can travel through multiple channels.

7. Data Center Certification

enfoTech Data Center receives the following certifications.

- **SSAE 16 (Statement on Standards for Attestation Engagements No. 16):** enfoTech Data Center is SSAE 16 SOC 2 certified that provide our clients an assurance that the security of the Center has met the highest standards to protect client’s data.
- **HIPAA (The Health Insurance Portability and Accountability Act):** enfoTech Data Center is HIPAA certified to help our clients to enhance Role-based security, audit data backup plan, strengthen user names and passwords, protect against malicious software, and more.
- **PCI DSS (Payment Card Industry Data Security Standard):** enfoTech obtains and maintains Payment Card Industry Data Security Standards (PCI-DSS) certification which is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of users’ personal information.
- **SSL (Security Socket Layer):** SSL (or known HTTPS) is a standard security technology for establishing an encrypted link between a server and a client (typically a website and a browser). It allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. To secure a website, enfoTech also applies Security Socket Layer (SSL) certified by **GoDaddy** to protect our website and make it more secure.

(B) Business Continuity & System Monitoring

enfoTech will continue monitor the system operation for good performance and respond to user requests. Our services include:

- **System Monitoring**
 - Monitor server daily to ensure good system performance.
 - Review system log daily to detect signs of system exception events, take proactive steps to investigate potential issues, implement changes, if necessary, to mitigate issues.
 - Perform real-time system and data backup to ensure business continuity. Backup will be automated at the servers with the following frequency:

SEQ	Description and Contents	Frequency
1	<ul style="list-style-type: none"> ▪ Primary hosting servers to Secondary hosting servers ▪ Entire server image is backup with incremental changes (partition, OS, systems, database) ▪ Hot fail-over between the Primary and Secondary servers to guarantee business continuity and no data loss ▪ Fail-over between the Primary and Secondary hosting sites are automatic 	Every 5 minutes Automatic
2	<ul style="list-style-type: none"> ▪ Secondary hosting servers to Tertiary hosting servers (different location) 	Every 15 minutes Automatic

SEQ	Description and Contents	Frequency
	<ul style="list-style-type: none"> ▪ Entire server image is backup with incremental changes (partition, OS, systems, database) ▪ The Tertiary hosting servers could be brought online within 4 hours if both the Primary and Secondary sites are down 	
3	<ul style="list-style-type: none"> ▪ Tertiary hosting servers to Quaternary hosting servers (another different off-site for security protection) ▪ Entire server image is backup with incremental changes (partition, OS, systems, database) 	Daily Automatic
4	<ul style="list-style-type: none"> ▪ System-wide full backup for all hosting sites and all servers ▪ Entire server image is backup with incremental changes (partition, OS, systems, database) 	Weekly Automatic

enfoTech utilizes Microsoft Hyper-V technology for replication and failover coordination. Application and database servers are preconfigured for automated failover from the primary to secondary site. While much of the failover process is automated, manual confirmation by the Recovery Execution Team (RET) is required to complete the transition.

When the primary site is restored, reverse replication synchronizes data and configurations, followed by failback to reestablish the primary as the main production site.

This Disaster Recovery (DR) design maintains mirrored environments of the production system at both secondary (DR-1) and tertiary (DR-2) locations, ensuring operational readiness in the event of any unplanned outage.

(C) Disaster Recovery

(C.1) Disaster Recovery Plan (DRP)

enfoTech also provides **Disaster Recovery Plan (DRP)** that defines the structured approach enfoTech will use to restore the EN Suite System in the event of a disruption. While the Business Continuity Plan (BCP) ensures overall continuity of operations, the DRP provides the detailed technical and procedural steps required to recover systems, data, and services following a disaster. The key objectives of this DRP are to:

- Ensure the rapid restoration of **the EN Suite System** operations following a disaster event.
- Minimize data loss through predefined recovery point objectives (RPO).
- Limit service interruption by meeting recovery time objectives (RTO).
- Protect the integrity and confidentiality of data during recovery.
- Provide confidence to Georgia stakeholders, and external partners that recovery actions are systematic and effective.

(C.2) Disaster Recovery Team

enfoTech's Disaster recovery activities are coordinated across specialized teams to provide coverage across technical, managerial, and operational areas:

- **Incident Response Team (IRT):**
Detects and reports disruptions, initiates logging, and escalates incidents to the Emergency Management Team.
- **Emergency Management Team (EMT):**
Holds the authority to declare a disaster, activate the DRP, and direct recovery operations. Serves as the central communication link with the State leadership.
- **Recovery Execution Team (RET):**
Executes failover procedures, restores systems at alternate sites, and validates service functionality.
- **Technical Services Engineers (TSE):**
Provide subject matter expertise in system troubleshooting, database recovery, and network reconfiguration.

(C.3) Disaster Response Procedures

enfoTech's Disaster response procedures provide the structured steps for declaring a disaster, activating this plan, and restoring critical **EN Suite System** services. These actions ensure rapid, coordinated recovery while maintaining transparency with stakeholders.

The Recovery Execution Team (RET) follows a structured checklist to ensure no steps are missed during recovery:

1. Confirm DRP activation by the Emergency Management Team (EMT).
2. Assess the status of primary, secondary, and tertiary facilities.
3. Determine the most viable recovery site (secondary, tertiary).
4. Validate backup integrity and replication status.
5. Initiate failover to the designated recovery site.
6. Restore applications, databases, and middleware services.
7. Verify security controls (encryption, authentication, access restrictions).
8. Test functionality with the Client stakeholders.
9. Document actions and update status logs.

enfoTech's Business continuity and disaster recovery are supported through:

- Redundant infrastructure across geographically separated data centers
- Regular data backups with tested restore procedures
- Defined RTO and RPO objectives aligned with business requirements
- Failover capabilities for critical systems
- Periodic disaster recovery testing and validation

These measures ensure continued service availability and data protection during adverse events.

(D) System Maintenance and Technical Support

enfoTech will provide maintenance and support to Client for the use of Systems delivered under the Project on an annual maintenance agreement renewable each year. Our maintenance services include:

- A. **Issue tracking and resolution:** enfoTech will host a web-based project team website (PTWS) to allow the Client users to submit service requests, report issues and track resolutions. The PTWS will provide the following mechanism for both parties to track resolution of service requests.

1. Issue report date	2. Issue description	3. Classification
4. Priority	5. Status	6. Plan Delivery Date
7. Complete date	8. Comments	9. Attachment

enfoTech will host conference calls with the Licensee on regular basis (initially once per month, and adjust the frequency based on the need). The call will include audio and visual components that provide easier communication on issues to allow enfoTech and the Licensee to review the PTWS issue list, prioritize service requests, review issue resolution progress, and schedule system release time.

B. Technical Procedures for Service Requests:

enfoTech will respond to the user’s service requests reported on the project team website (PTWS). Technical staff will acknowledge receipt of an issue within the allotted time per issue priority and provide technical services based on the priority jointly determined by the user and enfoTech.

1. Critical Priority: An issue classified as a “Critical” is a system error that prevents the user to use the Licensed program that is critical to the Licensee operations, and for which there are no known workarounds. Critical issue is system-wide error. Both parties will work together to reclassify the issue if enfoTech does not agree with the issue classification. If both parties agree the issue is a critical, enfoTech will respond to the issue in accordance with the resolution procedure listed below. An example is “Client cannot login EN Suite”.
2. HIGH Priority: An issue classified as “high” is a one that significantly effects the License’s capability to use the Licensed Programs and is not classified as a critical. High priority will cause one business process to break, but not a system-wide error. An example is “Client cannot issue a permit” for a permit type.
3. MEDIUM Priority: An issue classified as “Medium” is a one that effects the License’s capability to use the Licensed Programs and is not classified as a Critical or High priority. Medium priority will cause one incident to break, but not a process-wide error. An example is “Client cannot issue permit for one Facility”, but could issue similar permits for other Facilities.
4. LOW Priority
An issue classified as “low” is a user request that is not classified as critical, High, Medium priority. Low priority issue will not break a business process, but cause some inconvenience.

C. Resolution Procedures:

Upon notification by Client, enfoTech will respond to the Client Authorized Representative in the below response timetable when issue was reported to enfoTech. The response will include an estimated completion date for resolution. All time references shall mean Business Days from 9:00 a.m. to 6:00 p.m. Eastern Time.

Severity Level	Reporting Procedure	Response Time	Resolution Time
Critical	Emergency Hotline and record issue at	Within 2 hours if reported during Business Hours; within 2 hours of next Business Day if reported during off-	Within 6 hours if reported during Business Hours; within 6 hours of next Business Day

Severity Level	Reporting Procedure	Response Time	Resolution Time
	PTWS	Business Hours	if reported during off-Business Hours
High	Record issue at PTWS	Within 8 hours during Business Hours, within 8 hours of next Business Day during off-business hours	Within 5 days; or provide a work around/permanent fix agreed to by Client
Medium	Record issue at PTWS	Within 5 Business Days	Within 20 days, or included in next system release as agreed to by Client
Low	Record issue at PTWS	Within 10 Business Days	Within 40 days, or included in next system release as agreed to by Client

Response Time means the time enfoTech takes to acknowledge to Client that a newly reported issue is being investigated. If enfoTech cannot reproduce an issue, enfoTech shall request additional information from Client via phone call or email for which the SLA time will pause. If the issue is still not reproducible, authorized representatives of both parties shall negotiate in good faith the possibility of revising the target Resolution Time.

Resolution Time means the time that lapses between Client first reporting an issue to enfoTech and the time when enfoTech has resolved the issue or provided a work-around that is accepted by Client. If a temporary solution is provided, enfoTech will continue working on the issue for a permanent solution and keep the Client apprised of the progress.

The response or resolution time shall mean business hours (i.e., 9am to 6pm Eastern Time), which are Monday through Friday excluding holidays. For response time calculation, the time clock shall pause when enfoTech responds to Client service request. For resolution time calculation, the time clock shall pause when enfoTech provides a respond to Client including asking for Client’s clarification, or waiting for Client to verify system patch, or waiting for deployment of a system patch verified by Client.

D. System updates:

enfoTech will provide system maintenance releases. In general, there are two types of system updates.

1. **Emergency Patches:**

Provide emergency releases on an “as needed” basis. These patches are provided to address critical or certain high priority issues as mutually agreed by both parties.

2. **Maintenance Updates:**

Provide maintenance releases on a quarterly or semi-annual basis. Maintenance updates will address items that have not been included in the emergency patches and will be provided in a schedule mutually agreed by both parties.

E. Help Desk: enfoTech will provide a Help Desk hot line to the users for reporting system related questions and issues. Our standard service hours are from 9 AM to 6PM EST Monday through Friday, excluding holidays. When needed, Team conference calls can be used to streamline our technical support service.

(E) Quality Assurance for System Updates

enfoTech has implemented a comprehensive Capability Maturity Model Implementation (CMMI-Level 3) compatible mechanism for all projects. We have utilized all of the CMMI-Level 3 compatible procedures, project tracking forms, and collaboration processes for all our projects. We strive to achieve the following objectives:

- Standard processes for developing and maintaining software across enfoTech are documented, including both software engineering and management processes, and these processes are integrated and coherent.
- Standard processes are referred to throughout enfoTech's standard software process.
- Standard processes established at enfoTech are used (and changed, as appropriate) to help the managers and technical staff perform effective software engineering practices at enfoTech.

Since the software process is well defined, management has a good insight into technical progress on all projects. enfoTech's software process can be summarized as standard and consistent because both software engineering and management activities are stable and repeatable. Within established product lines, the cost, schedule, and functionality are under control, and software quality is tracked. This process capability is based on a common, corporate-wide understanding of the activities, roles, and responsibilities in a defined software process.

A Quality Assurance Plan is not a document *per se*, but a business process. In other words, the Quality Assurance plan is a process that is integrated into business practice throughout enfoTech to ensure that work output meets certain standard acceptance criteria.

enfoTech utilizes Visual Studio Team System as one of the tools to support our Quality Assurance Plan.

(F) Security to Protect Client's Data

enfoTech provides the following data security features for our IT infrastructure and data.

(F.1) Data Security

enfoTech provides the following data security features in its cloud hosting services:

- **Next-Generation Network Firewall Protection with Unified Threat Management**
 - Identity-centric enforcement for precise access control.
 - Built on a top-ranking Unified Threat Management (UTM) platform.
 - Intrusion Detection and Prevention (IDP) capabilities.
 - Comprehensive security policy definition, control, and management.
 - Highly effective IPS with over 10,000 signatures to block attacks that bypass conventional firewalls; behavior-based heuristics detect zero-day threats without existing signatures.
 - Secure Web Gateway to prevent access to malicious or inappropriate sites, ensuring a safe browsing environment.
 - Gateway-level Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control for intelligent, real-time protection against blended threats.
 - Continuous monitoring for anomalous data, with alerts generated if unauthorized data packets are detected.

- **Secure Remote Access**
 - Enables authorized users to access data from anywhere using hardware-based one-time passwords.
 - Provides network authentication, manages access, and enforces security privileges for remote connections.
- **Vulnerability Scan and Penetration Testing**
 - Conducted by a trusted third-party service.
 - Provides scanning reports quarterly or on demand, detailing vulnerabilities and mitigation measures.
- **Server Security Protections**
 - Applications are accessed through SSL/TLS-secured connections.
 - Network Load Balancer distributes traffic across up to 32 web servers, all communicating via SSL/TLS v1.2+.
 - Only a limited set of authorized personnel—including the Infrastructure Manager, Maintenance Manager, Release Manager, and Database Administrator—can access hosting servers.
- **Managed Anti-Virus**
 - Utilizes firewall-native hardware-based anti-virus protection.
 - Implements software-based anti-virus solutions for additional security.
- **Logging and Monitoring**
 - Records user log-ins/log-outs, transaction events, password changes, and security breach events.
 - Centralizes logs in a monitoring center and alerts relevant stakeholders of notable events.

(F.2) Data Encryption

The EN Suite system data is protected and central to enfoTech’s hosting strategy. Security measures cover all data states — at rest, in transit, and in use.

- **Data at Rest**

Stored data is protected using encryption technologies, access restrictions, and continuous monitoring. Sensitive datasets are secured on encrypted storage volumes, with additional safeguards such as role-based access and separation of duties to prevent unauthorized exposure.
- **Data in Transit**

To ensure secure transmission, all data moving between clients, applications, and hosting environments is protected using **SSL/TLS 1.2+ protocols**. VPN tunnels and private circuits are also utilized for inter-site and cloud communications, minimizing the risk of interception or tampering.
- **Data in Use**

Active data within the EN Suite systems is secured through operating system hardening, application-level controls, and strict session management. Monitoring tools validate ongoing system integrity, ensuring that data remains consistent and protected during active use.

(F.3) Access Controls

The EN Suite system adopts “role based” security module similar to the Windows operating system. The Security module is designed for ease of configuration, accuracy of security access, and audit trail.

The EN Suite system security is enforced through the use of Roles and Business Units. User roles are used to define data access privileges, for all users within a business unit, to modules, functionalities, and controls. A business unit is a functional group that defines the types of data and system functions the group should be interfacing with.

Client's data will be stored in a secured Data Center and no data access will be allowed. enfoTech project manager will grant limited access to employee under a need-to-know basis based on service requirements directed by the client project manager.

(G) enfoTech Admin Procedures to Protect Client's Data

- enfoTech maintains an Electronic Commerce Security Policy that every employee must comply
- All employee before starting working at enfoTech must sign an acknowledgement to consent that they have read, understand, and will comply with enfoTech security policies
- In addition, all employee working on the client's project must sign an additional acknowledgement to consent that they will comply with any security policies and procedures required by the client, before being granted access to the project related information.
- enfoTech enforces the Security Policy to protect our client's data through the following procedures:
 1. **Access Control:** Client's data will be stored in a secured Data Center and no data access will be allowed. enfoTech project manager will grant limited access to employee under a need-to-know basis based on service requirements directed by the client project manager.
 2. **Data Center Monitoring:** enfoTech is a Tier II Internet Service Provider. In addition to the software support services, enfoTech currently provides 6 professionals exclusively to monitor hosting environment. Jason Huang, enfoTech Executive Vice President has final responsibility of all hosting resources and directs all technical staff to support hosting tasks, monitor work load, and add additional resources if needed.

Our Data Center is being auto-monitored on 24x7 basis with a beeper alert to support personnel when an excursion occurs that will require human intervention. The support Team monitors server logs and respond to situation as necessary. Redundant servers, proactive monitoring, and skilled professionals enable us to provide 100% up-time since inception of our Data Center services.

We review our Security Policy annually and make necessary changes deemed required. If Policy is changed, new Policy will be communicated to all employees. All employee must provide written confirmation that they read, understand and will comply with the new Policy.

(H) Cost Management

Cost management is one of the essential tasks in quality project management. The enfoTech Project Manager will work with the client Project Manager to monitor project scope, deliverables, and spending to achieve a well-balanced project outcome. In addition, we provide the following management options to the client for cost management monitoring.

- **Not-to-exceed Cost Option:** we will propose a "not-to-exceed" project cost estimate, based on project deliverables defined for the project. enfoTech will commit to the project deliverables (in scope) under the estimated cost.
- **Change Request Management:** When there is a potential scope change, the enfoTech Project Manager will inform the Client Project Manager to explore resolution options. enfoTech will not engage in new work without written approval from the client Project Manager