INTERDEV PROPOSAL
Managed IT & Security Services

INTERDEV

IT | Security | GIS

TABLE OF CONTENTS

IT Services

INTERDEV SERVICE CATALOG

The following tables indicate the services included in InterDev's standard managed support services.

END USER SERVICES

Service functions that directly involve the support of the client End User. These services focus primarily on desktop hardware, application, training, monitoring, and management support. Inclusive of all work to be performed during normal business hours. Patch management and updates will be performed on a scheduled basis during a maintenance window. Service metrics to be measured will be specified in the client's agreement(s) that will cover this service.

SERVICE NAME	DESCRIPTION	FEATURES
Desktop Support	Provides in-person support for individual business users regarding end-user technology (hardware or applications)	• Onsite support for server & peripheral hardware • Remote hardware support • Incident Management • Problem Management
Application Support	Helping employees troubleshoot application errors or malfunctions (On-premise/Hosted/ Cloud)	• Remote application support • On-site application support • Incident Management • Problem Management
Mobile Device Support	Provides support for individual business users regarding mobile device technology (hardware or applications)	• Remote application and hardware support • On-site application and hardware support
Lifecycle Management	Standard management and administration of end user hardware and applications (On-premise/Hosted/Cloud)	• Version Control • Asset Management • License Management • Change Management
Patch Management	Patch and Firmware management of all end user desktop hardware and applications (On- premise/Hosted/Cloud)	• Windows Updates • Firmware Updates • Third Party Applications Updates
Monitoring	Proactive and reactive monitoring of end user desktop hardware and applications (On-premise/Hosted/Cloud)	• Device Monitoring • Limited Application Monitoring
Software Provisioning	Supply employees with necessary up-to-date software for them to work	• Request non-standard software • Procure/order new software • Install and upgrade standardized desktop software

DATA CENTER SERVICES

Service functions that directly involve the support of the data center operations and infrastructure. These services focus primarily on server and storage hardware, applications, monitoring, and management support. Inclusive of all work to be performed during normal business hours. Patch management and updates will be performed on a scheduled basis during a maintenance window. Service metrics to be measured will be specified in the client's agreement(s) that will cover this service.

SERVICE NAME	DESCRIPTION	FEATURES
Server and Storage Hardware Support	Provides in-person support for server and storage hardware regarding end-user technology (On-premise/Hosted/Cloud	- Remote hardware support - Onsite support for server & peripheral hardware - Incident Management - Problem Management
Server and Storage Application Support	Troubleshoot application errors or malfunctions (On-premise/Hosted/Cloud)	- On-site application support - Remote application support - Incident Management - Problem Management
Lifecycle Management	Standard management and administration of enterprise applications, server and storage hardware (On-premise/Hosted/Cloud)	- Asset Management - Version Control - License Management - Change Management
Patch Management	Patch and Firmware management of all end user desktop hardware and applications (On-premise/Hosted/Cloud)	- Hypervisor Updates - Windows Updates - Firmware Updates - Third Party Applications Updates
Monitoring	Proactive and reactive monitoring of server and storage related hardware and applications (On- premise/Hosted/Cloud)	- Device Monitoring - Application Monitoring
Data Backup and Recovery Management	Management and monitoring of all data backup and recovery systems. Includes any Data Backup and Disaster Recovery Policies and practices (On-premise/Hosted/Cloud)	- On-premise data backup management - Cloud data backup management - Data backup application support (on- premise or cloud) - Disaster Recovery application support (on- premise or cloud)
Facilities Management Support	Management and support of all data center facilities related infrastructure	- Access Control System Management - Power Systems Management and Monitoring - Cable Infrastructure Management - Environmental Control Systems Management and Monitoring
Hardware and Software Provisioning	Supply employees with necessary up-to-date software and hardware for them to work	- Request non-standard software - Procure/order new software - Install and upgrade standardized desktop software

NETWORK SERVICES

Service functions that directly involve the support of the network operations and infrastructure. These services focus primarily on network hardware, applications, monitoring, and management support. Inclusive of all work to be performed during normal business hours. Patch management and updates will be performed on a scheduled basis during a maintenance window. Service metrics to be measured will be specified in the client's agreement(s) that will cover this service.

SERVICE NAME	DESCRIPTION	FEATURES
Network Hardware Support	Provides in-person support for network hardware regarding network and telecommunication technology	• Onsite support for server & peripheral hardware • Remote hardware support • Incident Management • Problem Management
Network Application Support	Troubleshoot network application errors or malfunctions	• Remote application support • On-site application support • Incident Management • Problem Management
Lifecycle Management	Standard management and administration of enterprise-wide network hardware and applications	• Version Control • Asset Management • License Management • Change Management
Patch Management	Patch and Firmware management of all network related hardware and applications	• iOS Updates • Firmware Updates • Third Party Applications Updates
Monitoring	Proactive and reactive monitoring of network related hardware and applications	• Device Monitoring • Limited Application Monitoring
Facilities Management Support	Management and support of all data center facilities related infrastructure	• Access Control System Management • Power Systems Management and Monitoring • Cable Infrastructure Management • Environmental Control Systems Management and Monitoring

SECURITY SERVICES

Service functions that directly involve the support of the security team. These services focus primarily on security hardware, applications, monitoring, and management support. Inclusive of all work to be performed during normal business hours. Patch management and updates will be performed on a scheduled basis during a maintenance window. Service metrics to be measured will be specified in the client's agreement(s) that will cover this service.

SERVICE NAME	DESCRIPTION	FEATURES
Security Support	Security Engineer(s) Security Analyst(s)	• Remote Support • Incident Management • Problem Management
Firewall Management	Includes ensuring all appropriate services are enabled and configured, rules are configured in accordance with best practice, and performing regular backups of configuration	• Remote support • On-site support • Incident Management • Problem Management
Anti-Virus Management and Support	Configuration, Management, and monitoring of Anti-Virus / Endpoint Protection Platform to include ensuring complete coverage of AV/EPP in the environment	• Remote application support • On-site application support • Incident Management • Problem Management
Lifecycle Management	Administrative management of security related hardware and software specific to product lifecycle	• Version Control • Asset Management • License Management • Change Management
Patch Management	Patch and Firmware management of all security related hardware and applications	• Operating System Updates • Firmware Updates • Third Party Application Updates
Email Security Management	Configuration, management, and monitoring of email security platform.	• Remote support • On-site support • Incident Management • Problem Management

SUPPORT SERVICES RESPONSE

InterDev's ITIL based support structure for all support services is guided by our customer specific Service Level Agreements (SLAs) that are developed prior to the client onboarding process. InterDev will provide Crest Hill with 24x7 support options that include our basic and advanced monitoring services.

Service Levels and ResponseTimes

InterDev will work with Crest Hill to determine the most appropriate levels of support for each category of incident. This process will ensure InterDev's response is in sync with Crest Hill's expectations, business needs, and budgets. Defined SLAs are only valid during normal business hours, which are 8 AM to 5 PM EST Monday through Friday, unless otherwise agreed upon by InterDev and the client.

Urgency + Impact = Priority

An Incident's priority is determined by assessing its impact and urgency, where:

- Urgency is a measure of how quickly a resolution of the Incident is required
- Impact is a measure of the extent of the Incident and of the potential damage caused by the Incident before it can be resolved.

Incident Urgency (Categories of Urgency)

SERVICE NAME	DESCRIPTION
High (H)	The damage caused by the Incident increases rapidly. Work that cannot be completed by staff is highly time sensitive. A minor Incident can be prevented from becoming a major Incident by acting immediately. Several users with VIP status are affected.
Medium (M)	The damage caused by the Incident increases considerably over time. A single user with VIP status is affected.
Low (L)	The damage caused by the Incident only marginally increases over time. Work that cannot be completed by staff is not time sensitive.

Incident Impact (Categories of Impact)

SERVICE NAME	DESCRIPTION
High (H)	Many staff are affected and/or not able to do their job. Many customers are affected and/or acutely disadvantaged in some way. The damage to the reputation of the business is likely to be high. Someone has been injured.
Medium (M)	A moderate number of staff are affected and/or not able to do their job properly. A moderate number of customers are affected and/or inconvenienced in some way. The damage to the reputation of the business is likely to be moderate
Low (L)	A minimal number of staff (single user incidents) are affected and/or able to deliver an acceptable service but this requires extra effort. A minimal number of customers are affected and/or inconvenienced but not in a significant way. The damage to the reputation of the business is likely to be minimal.

A defined SLA structure increases our efficiency and effectiveness of dispatching tickets and getting them resolved in a timely manner. It also helps to set the City's staff expectations for when they can anticipate their incident or service requests to be filled. These levels can be modified if higher response levels are necessary for certain City services (i.e. Police, Fire, Emergency Operations.)

The finalized Priority Matrix for each Service Level or SLA layer would resemble the draft version below. The City's actual SLA's will be determined jointly between Crest Hill and InterDev.

		IMPACT		
		H	M	L
Urgency	H	1	2	3
	M	2	3	4
	L	3	4	5

PRIORITY CODE	DESCRIPTION	TARGET RESPONSE TIME	TARGET RESOLUTION TIME
1	Critical	30 Minutes	1 Hour
2	High	1 Hour	8 Hours
3	Medium	4 Hours	24 Hours
4	Low	8 Hours	48 Hours
5	Very Low	1 Day	1 Week

After Hours & Emergency Services

With our experience supporting municipalities we understand that local governments are 24x7 operations. InterDev will provide 24x7 support to Crest Hill that will include after-hours support that gets routed to our support call center. For after-hours support end users can submit emails or call a dedicated support number. Support request calls will go to a live operator based here in the US that will take note of their issues and do a live hand-off with their assigned technician or his/her backup. The Crest Hill staff will be directed to a technician and never be sent to a voicemail. In the case a technician cannot be contacted, the support call will be escalated to a manager.

The InterDev team is dedicated to providing the best response time for our clients. We adhere to the SLAs and strive to support our clients.

Advanced Security Services
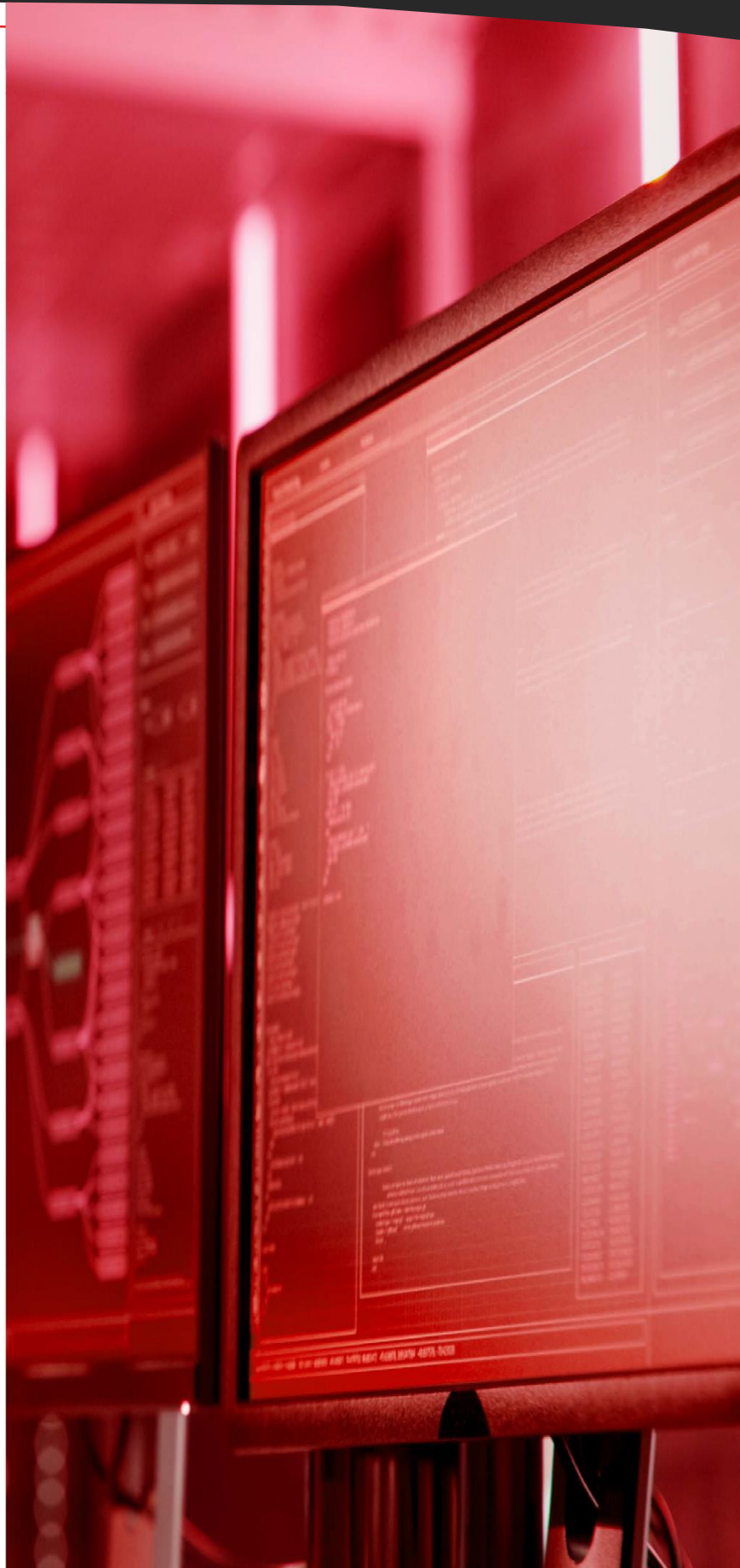
Advanced Security Services

Security has become an integral, necessary component of any organization. It no longer matters if you are a commercial entity or a public service organization, if you are large or small; security is a necessary part of conducting business. We believe that a well-constructed, layered defense, that is fully integrated into your systems and processes will serve as an enabler for your organization.

Conducting regular assessments, continually analyzing vulnerabilities, and testing those systems are critical components to any security program. Built specifically for these types of opportunities, InterDev has garnered a regional reputation for providing solutions-focused and industry leading managed IT services.

InterDev's deliberate approach to comprehensive IT solutions for government has prepared us to implement a strategy that will provide Crest Hill with the following benefits:

A. INCREASED OPERATING EFFICIENCY	B. INCREASED OPPORTUNITIES FOR COST SAVINGS	C. INCREASED FOCUS ON HUMAN CAPITAL
Will include increased capacity via an in-house IT team of professionals	Extensive experience working with municipalities to reduce costs and to become more efficient	Includes developed security services to benefit the City and the community
Reduced workload on in-house resources	InterDev's professional IT assessment provides critical data from your servers, PC workstations, laptops, network printers, cell phone, and camera systems to benefit the City.	Aims to support Crest Hill to improve the function of the City and the lives of residents
Increases a focus on compliance	Provide critical data for increasing equipment and product utilization, efficiency, and security of the City's environment.	Includes management of services to reduce security vulnerabilities, provide routine maintenance, and monitor overall infrastructure in developing an Information security framework
Increases the accuracy and vigilance around identifying and addressing malware events	No lost time due to system being unavailable. Reduced loss of time for minor incidents. Reduction in brand damage due to ransomware.	Security Program specifically for the City of Crest Hill.

InterDev Security Stack

Security Essentials – InterDev's proposed security package of products and services represents what we consider the absolute minimum level of security and risk management required for the City of Crest Hill. Our security stack will provide the City with a cost-effective set of security tools and represents what we would consider the minimum amount of due care to meet basic cyber-hygiene. The proposed security stack will include the following:

Patch Management – InterDev uses Ninja RMM as our system monitoring and patch management tool. InterDev will configure the patch management policies in concert with the client to find a balance between rapid deployment of critical patches with the least disruption to operations. Patch management includes operating system patches and a library of common third-party applications such as Google Chrome, Mozilla Firefox, Adobe, etc. Ninja also has the capability to provide image backups of servers and workstations as well as data backup capabilities.

Endpoint Detection and Response (EDR) - We have partnered with SentinelOne to provide an enterprise-grade, lightweight and highly effective endpoint protection platform with our high security configuration. This product is backed by a cybersecurity insurance product. We have witnessed this product stop browser-based web attacks in near real time. This is the security team's go-to tool when performing incident response to ensure an environment is fully protected. This offering comes in two variations to fit any budget.

Active Threat Hunting – InterDev has partnered with Huntress Labs to provide an active threat hunting agent that can find persistence mechanisms that anti-virus may not detect. It also provides external visibility for any exposed network ports that may present a risk and ransomware canaries that serve as an early warning that an individual system may be under attack. These canaries also act as a thumbprint if a breach ever occurs, we can use the canary to trace it back and determine what data may have been exfiltrated.

Email Security - Provided by Barracuda networks and hardened by our security team, this platform ensures that malicious email does not reach your users' mailbox. For our Office 365 customers, we also leverage Barracuda's Sentinel platform that leverages a behavior-based AI engine to prevent account take-over, auto-remediate phishing attempts and prevent domain spoofing.

Multi-Factor Authentication (MFA) - InterDev uses Duo Security for our three multi-factor authentication offerings. Duo MFA as a base offering, Duo Access for organizations requiring more granular control and conditional access, and Duo Beyond for those requiring much greater control over endpoints. Duo is completely cloud-based, easy to use and offers several methods for authentication.

Secure Internet Gateway and DNS-Based Protections – Cisco Umbrella's Secure Internet Gateway (SIG) and DNS filtering is one of the best strategies in defending against malware and protecting your assets as it detects potential malicious activity prior to the connection being established. It provides this protection whether on or off network and extends on-premises security and web filtering to your workforce, no matter where they are. The platform also provides visibility and control over risky applications as well as security scanning of your cloud environments.

Dark Web Monitoring - Using Kaseya's DarkWeb ID platform, the security team monitors and is alerted when your credentials are found on the DarkWeb allowing us to take pre-emptive action to protect against account compromise.

Password Manager – Credential harvesting an account compromise continues to be one of the most common methods for breach. Using a password manager can help users better manage their credentials without the need for memorization or the use of risky password files. Using a password manager will reduce potential exposure by instilling good password habits for your users.

Price Proposal
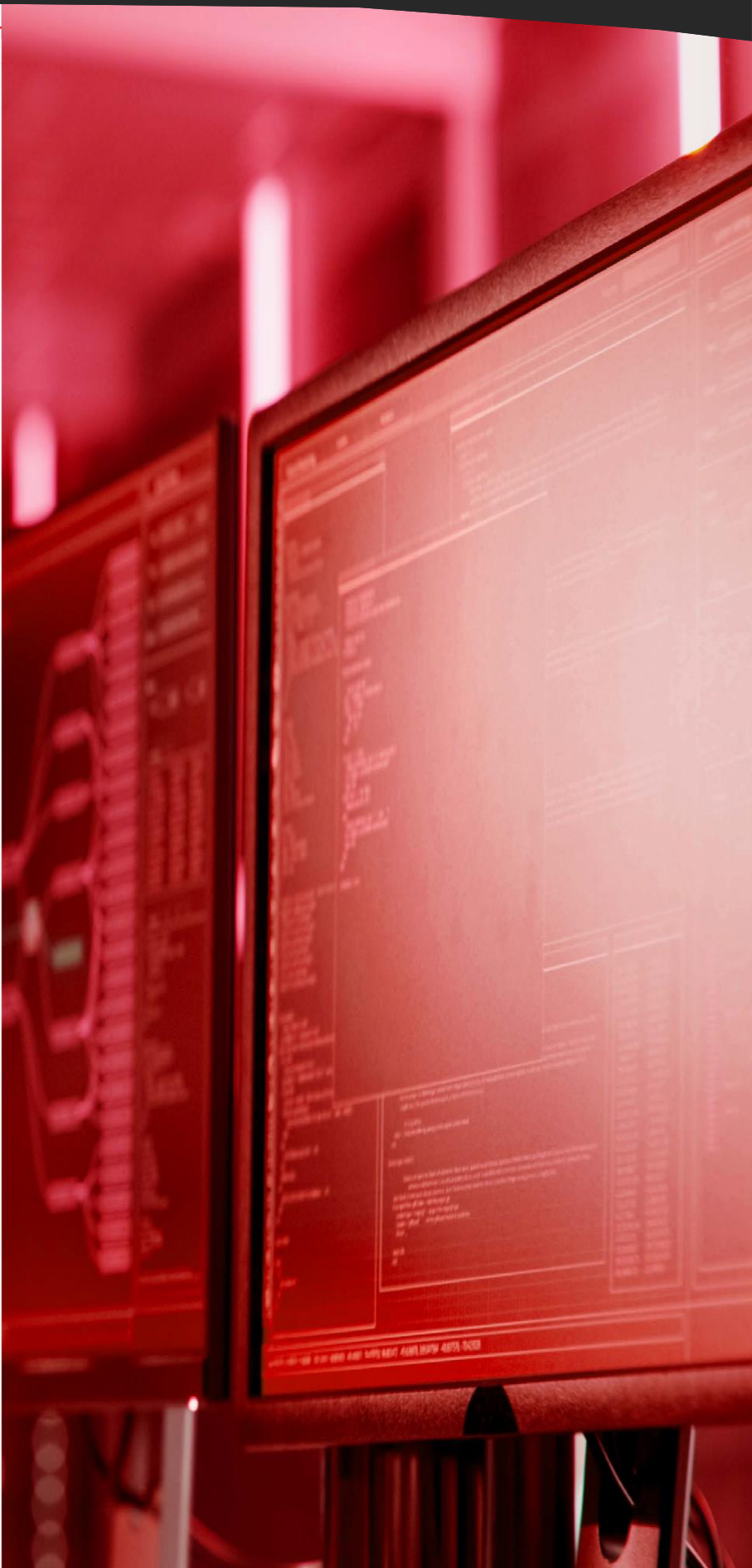
INTERDEV PRICING

OPTION 1 – Fully Managed IT & Security Services

DETAILED SERVICE PRICING LISTING		
STANDARD SERVICE CATEGORIES		**MONTHLY**
End User Services Data Center Services Network Services	**Full-Service IT Support** • Onsite Support Staff • 24x7x365 Support • Remote Sr. Engineering support • Remote Management & Monitoring Software	$17,609
ADVANCED SECURITY		
Advanced Security Services	**Security Essentials**** • Patch Management • Endpoint Detection and Response (EDR) • Active Threat Hunting • Total Email Protection • Multi-Factor Authentication (MFA) • Security Internet Gateway • Dark Web Monitoring • Password Manager	2,475
Monthly Cost		**$20,084**

Notes:

**The cost for the Security Services covers software plus administration from InterDev's Security Division and has been priced according to 60 users.

Pricing Adjustment "True Up" Schedule *- The IT Services fees are based off a per user and per device charge, which InterDev will perform a" true up" or adjustment of quarterly. The" true up" will adjust billing for the next quarter based on the total number of confirmed users by the City. The City of Crest Hill will only pay for the number of users that are active at the time of the" true up". If there is an increase in user count from the previous" true up" InterDev will only bill the City the difference for the last 30 days of services.*

Annual Escalator: Up to a 5% escalator shall be applied upon the agreement anniversary

Emergency Startup Cost *(One Time Cost)*	**Onboarding Tasks Include** • Management Configuration • Remediation prioritization • Password management • Agent Rollout • Network Monitoring Setup	$8,500

OPTION 2 - FTE & Security Services

FTE OPTION		MONTHLY
Full-Time Equivalent (FTE) Resource	**Systems Engineer*** • Dedicated onsite 40 Hour/Week	$15,000

ADVANCED SECURITY		
Advanced Security Services	**Security Essentials**** • Patch Management • Endpoint Detection and Response (EDR) • Active Threat Hunting • Total Email Protection • Multi-Factor Authentication (MFA) • Security Internet Gateway • Dark Web Monitoring • Password Manager	2,475
Monthly Cost		**$17,475**

Notes:

The FTE Option provides one (1) full-time resource. Additional resources will be billed hourly

**The cost for the Security Services covers software plus administration from InterDev's Security Division and has been priced according to 60 users.*

Pricing Adjustment "True Up" Schedule - *The IT Services fees are based off a per user and per device charge, which InterDev will perform a" true up" or adjustment of quarterly. The" true up" will adjust billing for the next quarter based on the total number of confirmed users by the City. The City of Crest Hill will only pay for the number of users that are active at the time of the" true up". If there is an increase in user count from the previous" true up" InterDev will only bill the City the difference for the last 30 days of services.*

Annual Escalator: Up to a 5% escalator shall be applied upon the agreement anniversary

Emergency Startup Cost *(One Time Cost)*	**Onboarding Tasks Include** • Management Configuration • Remediation prioritization • Password management • Agent Rollout • Network Monitoring Setup	$8,500

INTERDEV PROJECT STANDARDS

InterDev will consider any non-base services and/or tasks as a project that will be billed per the rate card within the proposal. All projects will be completed on a best effort basis as submitted by the client with an agreed upon schedule. Break Fix items do not constitute a project if the item is covered under the contracted base services.

InterDev will provide the following items below when engaging with the clients on any projects.

- Statement of work – Will contain a detailed list of what work will be completed with an overall estimate of hours of work and any overall cost estimates known or required in order to start the project process.
- Project Plan – This is a list of major milestones with estimated dates or span of time that constitute the whole of the project.
- Stakeholder Document – Will contain the list of approvers for each portion of the project. This could be financial approvers and/or timing or outage approvers.
- Project supporting documents – On an as needed basis, the project must be documented in order to provide knowledge transfer for ongoing support. Diagrams, Serial numbers, circuit ID's, and others will be placed here to formalize the project completion.
- Project closing – This will be a signed document certifying the approved completion of the project.

Projects requiring InterDev billing tracking: These must be approved by the Director and client, along with being tracked to document hours worked. This process is documented in a separate document stored by InterDev and maintained by InterDev but can be given to the client upon request.

PROJECT RESOURCES	RATES
CIO	$250.00
Systems/Network Engineering	$200.00
Security Engineering	$200.00
Project Management	$175.00
GIS Analyst	$175.00