LUZERNE COUNTY COMMUNITY COLLEGE
REQUEST FOR PROPOSAL
Managed Security Services

Section I. INTRODUCTION

Luzerne County Community College is seeking proposals from qualified Companies/Individuals to provide a comprehensive managed security solution including SOC, SIEM, and MDR services (see Section IV - Scope of Services for details). This document is a Request for Proposal (RFP) for the services described below and does not obligate LCCC to accept responses from eligible Companies/Individuals. The RFP establishes minimum requirements a Company/Individual must meet in order to be eligible for consideration as well as information to be included in the Company's/Individual's proposal.

Carefully examine the specifications, conditions and limitations. The selection of the successful Company/Individual will be made based on LCCC's evaluation and determination of the relative ability of each Company/Individual to deliver quality service in a cost-effective manner. The following specific criteria will be evaluated and must be addressed in the proposal:

1 Company/Individual History and Organization
2 Cost Proposal and Invoicing
3 Insurance
4 References

LCCC is not obligated to accept the lowest proposal and reserves the right to reject any and all proposals or amend the scope of the project. All of the Companies/Individuals must be duly licensed or otherwise have the ability to perform work in accordance with all governing local authorities and to the satisfaction of those authorities.

Notice of the Purchasing and Conflict of Interest Policies in place at Luzerne County Community College ("LCCC"):
Each owner/operator/individual/officer submitting a proposal or for whom a proposal is being submitted on behalf of the owner (each being referred to as a "Provider") to LCCC certifies that he/she/they are not a spouse, child, parent, brother/sister (each being referred to as an "Immediate Family Member") of any LCCC employee or Board of Trustee member at LCCC who owns more than a one (1%) percent ownership interest in the Provider/Provider's business.

If the Provider is an Immediate Family Member, according to College Policy and Procedure, disclosure must be made, and LCCC may decline entering into a business relationship with the Provider. Disclosure shall be made in writing at the time of submitting the proposal to the Director of Purchasing.

Violations of any of the policies or procedures may result in rejection of the proposal. Additionally, LCCC may have the right to recover damages suffered by LCCC in obtaining an alternative proposal, which damages may include, but are not limited to, consequential damages and reasonable attorney's fees.

Copies of these policies and procedures are available from LCCC upon request.

Under the Right To Know Law, the College is required to post to the PA Treasury Website all documents (BPO, PO, contract or agreement) for transactions valued at $5,000.00 and above.

Luzerne County Community College does not discriminate on the basis of race, color, national origin, sex, disability or age in its programs or activities. For a complete copy of the LCCC non-discrimination policy, contact the Human Resources Office at 800-377-5222, extension 7235. Inquiries may be directed to the Title IX Coordinator, John Sedlak, Dean of

Human Resources, LCCC, 521 Trailblazer Drive, Nanticoke, Pennsylvania, 800-377-5222 extension 7234 (jsedlak@luzerne.edu). Direct inquiries related to accessibility services for students to the Section 504 Coordinator, Rosana Reyes, Dean of Student Development and Enrollment Management, LCCC, 521 Trailblazer Drive, Nanticoke, Pennsylvania, 800-377-5222 extension 7243 (rreyes@luzerne.edu).

Section II. SUBMISSION OF PROPOSALS

Responses to this RFP are due by Noon on June 14, 2022. Late submittals will be rejected. All proposals are to be sealed, labeled with the subject of the proposal, and addressed to:
Luzerne County Community College
Purchasing Director, Mr. Len Olzinski
521 Trailblazer Drive
Nanticoke, PA 18634
Phone: 570-740-0370
The proposal submission may be mailed or delivered to the above address. Any questions regarding this RFP may be addressed to Trish Yencha, CIO, at 570-740-0412 or tyencha@luzerne.edu

Section III. CONTRACT TERM

The term of this contract shall be for a 1 to 2-year period, commencing on July 1, 2022 or thereafter, unless terminated by either party with thirty (30) days written notice.

Section IV. SCOPE OF SERVICES

- **Corporate Capabilities**
  - Please provide an audited copy of your company's financial statements for the past three years.
  - Indicate the number of years your company has been in business.
  - Indicate the number of years your company has offered each of the services in the MSS/MDR portfolio.
  - Where is your company headquartered? Indicate how many security operation centers (SOCs) you have, and where each one is located.
  - Do you have venture capital or other funding supporting your MDR business?
  - What percentage of your security service revenue for the trailing 12 months is from MDR? What percentage is from security professional services or consulting?
  - What percentage of your company's revenue is spent on MDR research and development (R&D)?
  - Describe all documented policies, procedures and audit requirements that will ensure maintaining the privacy and confidentiality of LCCC data from the data of your other customers.
  - Describe alliances with other companies you have that are related to your services, such as using a third-party software as part of your MDR portfolio.
  - Please provide an overview of your plans for continuity of service to LCCC.
  - Provide evidence of up-to-date business liability insurance.
  - List any recent awards your company has received.
- **Qualifications and Staffing**
  - Experience
    - Indicate how many MDR customers you have.
    - Please provide three references in LCCC's industry or market sector that are of similar size to LCCC. Include name, title, email, and phone number.
    - Personnel Infrastructure
    - Does your organization typically subcontract staff or do you maintain internal resources to meet the needs of your clients? If you subcontract, what contingencies do you put in place to ensure sufficient resources are available at all times during the contract?
    - Indicate the total number of employees in your company, and the number of employees responsible for MDR delivery.
    - Please describe the relative distributions of employees in your MDR company providing delivery, project management, customer service, and how these employees are geographically distributed.
    - What is the ratio of monitored security devices to personnel?
    - What is the average employment time of an MDR analyst within your company?

- Analyst Qualifications
  - What percentage of your staff has security certifications (list the certifications), and what is the average number of years of experience they have in performing security monitoring or security consulting?
  - Provide a sample job description and/or resume for your security-monitoring staff. Include a summary of the technical expertise and/or special capabilities required.
  - Do you hire different levels of analysts? If so, what are the minimum requirements (years of experience, education, types of skills) for each level?
  - Explain the process of initial and ongoing training of your security-monitoring staff.
- Analyst Vetting Procedures
  - Please describe the citizenship requirements per geographic location and/or per security operations center for governance purposes.
  - Describe the process for screening and hiring your staff for MDR.

- **Service Methodology**
  - Service Overview
    - Explain the level of customization you can offer with your security plan. What steps will you take to understand the LCCC environment in order to make informed recommendations?
    - Provide a brief overview of your managed security services and any supporting products.
    - "Describe the architecture of your MSS delivery capability, including elements in your SOC, data center (on your premise, colocations, and private and public cloud services), network and our premises, as well as the centrally delivered log management, analytics and portal tiers, and capabilities for collecting event logs and data from other locations (e.g., software as a service [SaaS] and infrastructure as a service [IaaS]).
    - Provide example architectural diagrams and descriptions. Indicate where there are any regional differences in architectures or technologies used. Finally, include and identify any elements that are delivered by third-party partners."
    - Describe your support for monitoring security or other related events from SaaS providers such as SalesForce (SFDC), O365 and Azure AD. List which providers can be monitored natively. Do you require and/or support cloud access security brokers (CASBs)?
    - What types of LCCC owned systems would you typically integrate with your MDR/MSSP offering?
    - Where would the technology required as part of this contract reside -- LCCC facilities or your MDR/MSSP facilities?
    - Who will LCCC work with in the delivery of the Service? Who will be our primary point of contact? (Include roles, responsibilities, expertise)
  - SOC
    - Is your SOC(s) staffed 24x7x365?
    - Do you maintain full, dedicated Security Operation Centers (SOCs) to support your MDR/MSS?
    - Do you own and manage your SOCs?
    - Where are your SOCs located?
    - Describe your available levels of SOC redundancy.
    - Describe how you limit service interruption if a SOC goes offline.
    - Describe security safeguards around the SOCs.
    - Describe the staffing for each of your SOCs.
    - Do you permit an onsite SOC visit? If so, what is the process for planning the visit?
    - What are your top technology investment areas for a SOC?
  - Customer Notification and Support
    - Please provide an overview of your customer notification and escalation process. Include details on how often a customer is notified of a security event, and on the methods of notification.
    - What channels are there for LCCC to be alerted to potential security incidents or request support?
    - Indicate the frequency of meetings or teleconferences to review performance, issues, threat environment and responses. Explain the types of analyst and account management support provided during those meetings.
    - Describe the process should LCCC have a complaint.
    - Describe your customer support tiers, including the capabilities and location of staff at each tier.
    - Describe your problem resolution and escalation procedures.

- Service Level Agreements
  - Indicate device/agent management and real-time event management notification service levels. Explain how they are measured, and how they will be communicated to LCCC.
  - Provide a sample of an SLA as outlined in the scope, in addition to the service onboarding and delivery phases.
  - Describe your SLA performance reporting. If applicable, indicate whether these methods are used in some or all regions.
  - Indicate your process for notifying us of your noncompliance with the SLA, and vice versa.
  - Describe the remedies available to LCCC should you fail to meet any SLAs. Explain any regional variations to remedies.
- Legal Requirements
  - What access to internal-auditing documentation will you provide if our auditors, customers or business partners require this documentation in support of legal, regulatory or contractual requirements? What is your process for requesting documentation? What are the time frames to which you will commit for producing documentation?
- Termination
  - Outline early termination penalties and charges. Describe how the costs are calculated to extract all captured data to be moved to another MSSP, if applicable?
  - Describe how LCCC's data would be obtained during the termination process.

- **Implementation**
  - Delivery
    - List the primary tools used to deliver your services. Describe the function or service offering they support, and indicate whether they are proprietary, commercial, or open source, for example, log collection, log management and storage, analytics, reporting, case management and workflow, and incident response.
    - Will your services require the use of proprietary technology that LCCC must purchase or install? If so, please list all pertinent information related to this technology, including hardware, software, networking, middleware and database requirements. Include any associated costs as a separate line item in your quote.
    - Indicate how your services will be delivered in our internal virtual infrastructure. Include details about how the services will accommodate the scaling (larger or smaller) of the virtual environment, the implications for technology deployment to support monitoring, and related contractual, license or cost implications.
    - Indicate how your services will be delivered in an external or public cloud infrastructure. Include technology and contractual or licensing requirements related to provisioning, ongoing monitoring and de-provisioning of services to the cloud infrastructure. Describe the process to add or remove monitoring sources in a public cloud infrastructure.
    - Explain how you will complete an initial assessment, and how you will establish a baseline security level. Include specifics on your implementation timeline; infrastructure requirements; data transfer, data storage and segregation, and backup systems; and encryption standards.
    - Based on the information that has been provided, what do you see as the approximate overall duration to transition to fully operational MDR monitoring? Provide a timeline with your underlying assumptions in order to commence the service.
    - Describe the frequency and opportunities for continuous improvement during the implementation phase.
    - Integration
      - Explain how these services, and any supporting products will use or interface with products LCCC has in place. Ensure that you include details on how you intend to connect to LCCC's infrastructure to provide support.
      - Describe integration capabilities with enterprise directories, and configuration management databases (CMDBs). Explain how these integrations support the delivery of your services.
  - Future Changes
    - Describe the process for adding services or new technologies. For example, if we acquire new assets, adopt a new cloud application, or make architectural changes to the environment — how

would this be supported and incorporated into an SLA?
        - What process will determine if a change is within the original scope of the supplied technology or a new feature? How will the costs be determined?

- **Security Event Monitoring**
    - Capabilities
        - Explain your methodology for detecting unknown threats.
        - Indicate the capabilities of your services to monitor our firewall, intrusion detection system (IDS), intrusion prevention system (IPS) and vulnerability data. Specifically Sophos Firewalls, Microsoft Defender for Endpoint and Barracuda Web Security.
        - Please describe how your team uses signature-based and correlation rules.
        - Besides the use of advanced analytics, do your MDR analysts use other methodologies to hunt threats? If so, detail why and how.
        - Explain your ability to analyze this data and to provide real-time event correlation between data sources, and real-time alerting of security incidents and system health incidents.
        - Explain how your company keeps signatures/rules updated versus future threats.
        - Explain support for the creation and management of customized correlation rules. Explain the capabilities available to our staff for doing so. Describe any limitations, such as data sources, age and query frequency.
        - Explain your ability to analyze this data to identify when changes in behaviors of users or systems represents risk to our environment.
        - Explain your methodology for detecting custom or targeted attacks directed at our users or systems.
        - Can custom alert rules be configured for specific events (e.g., Admin logins to specific applications during specific times of day)?
        - What mechanisms would you use to detect for use of zero-day exploits or ransomware infections?
    - False Positives
        - Explain your methodology for reducing false positives and false negatives and for classifying security-related events that represent a risk to LCCC. What is your false positive rate?
        - Describe how false positives are managed, and how your company will incorporate false positive feedback from LCCC.
    - Workflow
        - Describe the typical workflow and process that occurs when your detection analytics alerts on an event, beginning with how that is presented to a SOC analyst for evaluation, through the triage, validation, prioritization and customer alerting/notification process. Indicate which steps in this cycle are automated versus manually performed by analysts.
        - Explain the expected working relationship, roles and responsibilities between your security staff and LCCC's security staff when assessing, investigating, and responding to incidents.
        - Please provide an example of how your services detected and addressed a recent security incident.
- **Security Risk Management**
    - Log Management
        - Describe the service capabilities to execute and analyze vulnerability scans internally and externally with the organization
        - Indicate the technologies used to conduct scans, both commercial and open source.
        - Provide details on your methodology for collecting and analyzing vulnerability and asset data (e.g., configuration) from all sources in scope.
        - Describe the process by which vulnerabilities are triaged and prioritized prior to reporting, including the integration of previous scan results and actions carried out. Is the vulnerability management (VM) data also used in the same fashion for MDR services, if applicable?
        - Describe integration capabilities with vulnerability assessment data, including how the vulnerability data is used in support of triaging and investigating potential security events, and alerting and reporting capabilities.
        - How can vulnerability scans be scheduled, initiated/managed via your portal? How are results viewed in the portal?

        - Indicate the frequency your MDR can scan our environment.
        - How frequently is the vulnerability database updated, and what are the data sources used for that?
        - Indicate the application-specific scanning that you carry out as part of your VM services.
- **Security Device Management**
    - Questions
        - Indicate the capabilities of your services to manage our security technologies in scope.
        - Explain your process for updating software to include signature updates and system patches. How do you ensure that this is done in a non-intrusive manner to your customers?
        - For device management services, indicate whether changes are reviewed to assess increased risk, exposure or the effects on capacity.
- **Security Information Management**
    - Log Management
        - Indicate the data sources supported for log collection, reporting and retention. Can logs be collected from any source? Describe the collection methods (e.g., forwarded syslog, Windows Management Instrumentation [WMI], local forwarding agent).
        - Will all of our raw event logs and data be collected and forwarded to your platform for storage? If no, describe the variation and options for full log event retention (if applicable).
        - Will our logs be compressed and encrypted in transit, and is it a guaranteed delivery via a store and forward type of solution? If so, please describe.
        - Indicate any limitations to your log collection capabilities, such as peak event rates, volume or sources.
        - Explain the capabilities that allows LCCC staff to search and browse original log data. Describe any limitations to this capability.
        - What is the process for adding additional log sources to the scope of service? Include the implications for deployment architecture, integration costs and ongoing costs.
        - Explain the capabilities of LCCC staff to create and modify reports based on collected log data. Indicate any limitations, such as number of reports, complexity of queries and age of data.
        - How do you perform monitoring of off-premises infrastructure and software?
        - Will our log data be held on a multi-tenant system or a stand-alone system?
        - What controls are in place to secure our log data? (e.g. encryption, access controls, logging, etc.)
    - Data Collection
        - What LCCC data will be collected/captured by the MDR service. Where is that information stored? How is the information backed up and where is it typically stored? Detail use of hot sites, warm sites, or cold sites, as well as your disaster recovery capabilities.
        - Data Storage and Customer Access
        - Specify how your company approaches the online/warm/cold types of storage.
        - Are systems and storage dedicated to a particular client, or is the system shared between multiple clients?
        - At the end of any contract period, would LCCC be able to retrieve all its data from your MDR/MSSP services?
        - Would LCCC have read-only remote access to LCCC-owned log data on the MDR/MSSP SIEM systems to allow for incident management, data analysis and visualization, or is access restricted to MDR/MSSP service staff only?
    - Data Retention
        - Indicate your standard data retention policies and ability to modify them to meet our business & compliance requirements.
        - Is there a minimum and maximum of times that log retention can be offered? Describe what is actively available versus what is kept offline. If 365 days of storage is required, how will that be priced for LCCC?
        - How much data is typically retained by the MDR/MSSP (i.e., size limitations and length of time)?
    - Information Security
        - Do you monitor your staff compliance to information security policies and procedures?
        - Indicate any industry certifications/attestations your security operation centers hold, such as Statement on Standards for Attestation Engagements (SSAE) 16 Type 2, or International

Organization for Standardization (ISO) 27001. If so, please provide evidence.
        - "Describe how LCCC's data (including data generated by your company about security events and incidents affecting LCCC will be governed and protected in transit. Consider this from a technology perspective, as well as via processes and procedures.
        -
        - How will the treatment of LCCC's confidential data assist with better job performance (e.g., creating internal architecture and topology maps)?"
        - Provide examples of how your company has met specific regulatory or statutory requirements to the data within specific geographic or political boundaries. Provide answers only for regions or specific countries where there is concern.
        - What regulatory regimes and frameworks do you comply with? Please confirm which of these you also support for your customers.
- **Advanced Analytics and Capabilities**
    - Advanced Analytics
        - Explain the context around user and asset activity that your solution can provide.
        - Do you offer more than one approach to threat detection? Please elaborate.
        - Describe any managed detection and response-type service offerings (e.g., managed endpoint detection and response, threat hunting, remote response and containment).
        - What technologies are used to enable advanced analytics?
        - How do you profile and monitor entity and user activities and behaviors (e.g., user and entity behavior analytics [UEBA])? Describe specific approaches and models/algorithms used, including any regional variations.
        - Describe your ability to implement watch-lists, both those you define, and those we define.
        - Describe your use of predictive analytics, including specific approaches and models/algorithms used, and any regional variations.
        - Describe any specific network monitoring and/or network forensics features, capabilities or offerings to detect advanced, targeted attacks.
        - Describe any specific payload analysis features, capabilities or offerings to detect advanced, targeted attacks.
        - Describe any specific endpoint behavior analysis and/or endpoint forensics features, capabilities or offerings to detect advanced, targeted attacks.
        - How is streamed data with real-time advanced analytics supported? Describe and list any technologies supported (e.g., Kafka, NiFi).
        - Describe the data and threat visualization capabilities available to us via any available portals.
    - Big Data
        - Explain if/how you leverage big data platforms for the collection, retention and analysis of large volumes of operational and security data for analysis.
        - How are big data platforms used to support the collection/analysis of network and endpoint data?
        - Does your company require the deployment of its own network data collection/analysis solution?
        - Can your company use Microsoft Defender for Endpoint, or is it mandatory that LCCC use your company's EDR solution?
    - Information Sources
        - Explain how you use external data (e.g., threat intelligence feeds) to analyze potential threats to LCCC's environment, and describe what access to this data LCCC will have.
        - What sources of information do you use for threat intelligence? Does this also include dark web coverage?
- **Portals, Reports, Dashboards**
    - Portals
        - Indicate any local language support or localization features in your portal, and note any regional differences.
        - Describe the information provided by and features available through the web-based portal or console associated with your services. Describe the underlying technology (HTML5, Flash, JavaScript, etc.).

        - Include details on your support for role-based access control (RBAC), customization of screens and data presentation, predefined correlation rules, and predefined reports.
        - Indicate whether all services and MSS features, including those delivered by partners, will be available via a single portal, regardless of region or part of business delivering the services.
        - What authentication and identity management system does your portal use? Do you provide support for federated identity management (FIM)?
        - How does the portal provide us access to external threat intelligence feeds, in addition to LCCC's own threat intelligence feeds?
        - Describe support for bidirectional threat intelligence using open standards, such as STIX/TAXII/OpenIoC.
        - Can LCCC access, and search log event data via your MDR/MSS customer portal?
        - Describe how user access to data and reports can be restricted based on role and group.
        - "Describe any integration capabilities with third-party service desk and ticketing tools and services. How is this achieved (e.g., email, application programming interfaces [APIs], etc.)?
        - Also, indicate if you provide single-direction or bidirectional support, and whether the integrations are subject to additional costs."
        - Describe the portal capabilities to enable our staff to create, update and close tickets.
        - Describe how much visibility your company provides on the tasks of the workflow. Consider how many alerts there are, your staff level (e.g., Tier 1, Tier 2, Tier 3), and how long they are on a particular phase in the process.
    - Reports and Dashboards
        - Please describe your ability to access reports, documents, and other information directly from your solution's platform.
        - Describe operational, regulatory and executive reporting capabilities.
        - Indicate the number of predefined reports, including specific regulatory and compliance items supported, that will be available for LCCC. Please provide examples.
        - Explain how report data can be exported to or used by an external report writer or risk dashboard.
        - Explain the capabilities for our staff to create customized, ad hoc queries and reports. Describe any limitations to ad hoc query or report generation, including data sources, data age and query frequency. Provide the timeframe for turnaround of ad-hoc reporting.
        - Describe your standard reporting process. How frequently will we receive standard reports? Do you have a web-based reporting capability? If so, provide sample reports and screenshots of the interface.
        - Do you have asset-based reporting allowing LCCC to create and group assets, assign criticality and view event, scanning and all other information using asset views?
        - List the various formats reports can be created in. Can they be sent securely via email?
        - What is your approach to providing meaningful security metrics? Describe reports available in the portal that LCCC can be use to demonstrate security effectiveness and ROI.
        - How is your reporting interface structured? Do we use multiple interfaces for different services? Is the information integrated across product & service lines? What cross-service line metrics and reports do you offer?
        - Can we create custom reports? How is this accomplished?
        - What pre-built reports are available? Are there compliance reports? If so, which regulations are supported?
- **Pricing and Contracts**
    - Pricing
        - Indicate and describe the licensing model(s) for your MDR/MSS offering.
        - Indicate and describe the pricing model for managing/monitoring virtualized security devices or log sources.
        - Provide the base cost and pricing methodology.
        - Please indicate details on the number of devices or data sources (e.g., IDS sensors, firewalls and servers) that are included in the cost.
        - Is pricing differentiated according to the sophistication of analytics used?
        - Provide a detailed breakdown of one-time costs versus recurring costs.
        - Is there a minimum commitment for particular usage, total volume, individual spend or

aggregate spend in order to receive the rates and terms provided in the proposal? If so, explain.
        - Provide any licensing and warranty information for third-party products you may require LCCC to purchase in support of this service.
        - Indicate the discounts available, based on volume of services and contract length.
        - Is pricing differentiated according to service tiers or direct access to security engineers?
        - Indicate any consulting support hours built into your standard MDR/MSS contracts.
        - Indicate hourly or daily pricing for additional consulting hours we can purchase during the MDR/MSS engagement.
        - Are there any additional fees for incident response support or digital forensics services (e.g., if onsite deployment of personnel is required)?
    - Service Changes
        - How do new technologies get factored into the ongoing costs of the contract?
        - How are changes to the services factored into the ongoing pricing? For example, can devices or data sources be added to the contract without affecting pricing or services?
        - How will the MDR/MSSP cope with an increase or reduction in our infrastructure architecture during the contract term? What are the implications on contract costs?
    - Contracts
        - Please provide the name, title and appropriate contact information of the authorized negotiator or contract-signing agent.
        - Please explain in detail your contract liability limitations — is this limited by the price of the paid contract?
        - How long will the proposal remain in force from the date of submission?

V. INSTRUCTIONS

Responding Companies/Individuals must address the following subjects in their proposal:

1. Company/Individual History and Organization

Provide a brief history including brief biographical information regarding the personnel who would be directly responsible for the service.

2. Cost Proposal and Invoicing

Please provide all subscription, licensing and Implementation Costs as detailed in Section IV. Seeking a 1 to 2 Year contract billed monthly or annually.

3. Insurance (Companies/Contractors only, does not apply to individuals)

The successful provider shall carry and maintain, with respect to any work or service to be performed at LCCC facilities, insurance written by a responsible insurance carrier, to provide for the following:

- Workers' Compensation as required by applicable statute and Employer's Liability Insurance.
- Commercial General Liability Insurance in the amount of $1,000,000 listing the College as additional insured
- Automobile Liability
- Include a copy of Certificate of Insurance including limits with the response.

4. References

Provide at least three (3) client references whose facilities are comparable in size and profile to Luzerne County Community College. Include company name, address, contact person and contact number.

Luzerne County Community College would like thank you in advance for your interest in participating in this request for proposal. If for some reason you are unable to submit a proposal to the College, please let us know the reason why so you will remain on our active bidders list for the future.
Fax to 570-740-0525.

You can also e-mail your reason for non-participation to lolzinski@luzerne.edu so that we can keep it in our file.

Subject: PA Act 153 - Background Clearance Requirement

Act 153 – The Pennsylvania state legislature sought to strengthen protections for children in the PA Child Protective Services Law. The law went into effect on December 31, 2014 and now requires colleges and universities to obtain background clearances for any individual having routine interaction with children at the college or in a college-sponsored program, activity, or service. This requirement applies to college employees, volunteers, independent contractors, and students. This law requires mandatory reporting of suspected child abuse directly to the PA Department of Human Resources.

All Contractors will be required to obtain the three (3) mandatory background clearances: 1) PA Criminal Background, 2) PA Child Abuse History, and 3) FBI Cogent Clearance Fingerprinting.

These clearances must be provided for all contractor representatives/employees who will be on the campus of Luzerne County Community College to perform the work awarded. If you are unable obtain these state required background checks, you will be ineligible to perform work at the

College.

Below are the following required clearances and instructions to obtain them.

1. **Act 34 - PA Criminal Background (**On-line)

   Results are usually instantaneous. Make sure you hit "yes" to get a copy.

   Provide copy to the Human Resources Office

   https://**epatch**.state.pa.us/ Cost $22

2. **Act 151 - PA Child Abuse History** (On-line)

   Results are mailed or can be viewed and printed at the website.

   Provide the original clearance document to the Human Resources Office.

   Attached for your reference is a file which contains directions on navigating through the website.

   Google Chrome - https://www.compass.state.pa.us/cwis Cost $8

3. **Act 114 - FBI Fingerprinting -** IdentoGO (On-line)

   Register on-line by selecting Digital Fingerprinting. Enter the Service Code 1KG756. Submit your registration number to the Human Resources Office.

   https://www.identogo.com/locations/pennsylvania Estimated cost - $22.60