State of Utah

SPENCER J. COX
Governor

DEIDRE M. HENDERSON
Lieutenant Governor

Department of Government Operations
Division of Technology Services

MARVIN DODGE
Executive Director, DGO

ALAN FULLER
Chief Information Officer, DTS

PHILIP BATES
Director, Utah Cyber Center - CISO, DTS

UCC-SLCGP-001

MEMORANDUM OF UNDERSTANDING BETWEEN THE UTAH CYBER CENTER AND THE GREATER SALT LAKE MUNICPAL SERVICES DISTRICT

FROM: UTAH CYBER CENTER

TO: GREATER SALT LAKE MUNICIPAL SERVICES DISTRICT

SUBJECT: Participation in the State and Local Cybersecurity Grant Program Statewide Projects

Representatives from the State of Utah, City and County Governments, School Districts, Universities, and critical infrastructure, who together form the Utah Cybersecurity Commission, collaborated to develop a State of Utah Cybersecurity Plan that outlines specific goals and objectives related to cybersecurity in Utah. These goals and objectives focus on improving the sharing of information critical to cybersecurity operations, providing access to cybersecurity resources and education, developing a whole-of-state approach to cybersecurity, mitigating risks associated with cyber attacks, enhancing preparedness, and improving the ability to respond to incidents.

The complexity and prevalence of today's cybersecurity threats highlight the need for State and Local governments to work together to accomplish the goals and objectives of the plan. As we continue to develop cybersecurity capabilities, we must remain dedicated to improving the resilience of Utah governments, across jurisdictional boundaries, assisting each other as we grow. This Memorandum serves to outline specific interactions between the Utah Cyber Center and Local Government Entities in relation to the Statewide Projects established in the plan.

Section 1: Purpose

The purpose of the State of Utah Cybersecurity Plan is to:

- Improve the sharing of information critical to cybersecurity operations
- Provide access to cybersecurity resources and education
- Develop a whole-of-state approach to cybersecurity
- Mitigate risks associated with cyber attacks
- Enhance preparedness
- Improve the ability to respond to incidents

The Plan accomplishes these purposes by providing tools and resources to local governments that may be too expensive to procure on their own through use of funds from the State and Local Cyber Security Grant Program. This MOU outlines how the tools and resources will be implemented, what responsibilities both the LGE and UCC will bear, and how these parties should interact in the execution of these projects.

Section 2: Scope

The scope of this MOU for the State of Utah Cybersecurity Plan Statewide Projects includes the Utah State Government (as represented by the Utah Cyber Center), as well as:
The Greater Salt Lake Municipal Services District

Section 3: Definitions

As used in this MOU:

- **"Global Administrator"** means administrative users that have access to administer across all accounts.
- **"KB4"** means KnowBe4
- **"Local Government" or "LGE" (Local Government Entity)** means the same as that term is defined in 42 U.S. Code § 5122(8).
- **"MDR"** means Managed Detection and Response
- **"Project 1" or "MDR Project"** means the MDR for LGE's project as outlined in the State of Utah Cybersecurity Plan.
- **"Project 2" or "Vulnerability Management Project"** means the Vulnerability Management project as outlined in the State of Utah Cybersecurity Plan.
- **"Project 3" or "Security Professional Training"** means the Security Training Course project as outlined in the State of Utah Cybersecurity Plan.
- **"Project 4" or "Security Awareness Training Program"** means the Security Awareness Training as outlined in the State of Utah Cybersecurity Plan.
- **"S1"** means SentinelOne
- **"Saved Query"** means the S1 console feature called Saved Query that can be used to create custom threat hunting queries that can be executed against all previously recorded endpoint telemetry. This is an unlimited resource.

- **“SOP”** means Standard Operating Procedure
- **“STAR Rules”** means the S1 console feature called STAR rules that are used to create custom threat hunting queries that are run against all endpoint telemetry, including incoming data. This is a limited resource.
- **“The Plan”** means the State of Utah Cybersecurity Plan that was created for the State and Local Cybersecurity Grant Program (SLCGP)
- **“UCC”** means the Utah Cyber Center as defined in Utah Code 63A-16-1101.

Section 4: Project Details

Project 1 - MDR Project

Participation in this project places no financial or contractual obligation, beyond what is defined in this MOU, on the LGE. This service is being provided to LGEs at no cost for the project period of 10/31/2023 through 12/31/2027. This MOU and MDR service will automatically terminate at the end of that period (12/31/2027). Should the LGE wish to discontinue use of this MDR and terminate the MOU sooner than the defined end date of the project, the authorizing official of the LGE will need to notify the UCC in writing no later than three weeks prior to termination.

S1 console data, including endpoint telemetry will be stored in an S1 cloud-hosted environment, operating in AWS U.S. West. Each LGE will have their own account that is visible only to their staff, Global Administrators, and S1 Staff. Each LGE can build and configure their account however best suits their needs. LGEs will have full administrative rights to their accounts.

UCC staff will be the only entity assigned Global Administrator access. UCC will not perform any actions inside of a LGE account without the LGE expressly requesting the action be taken. UCC, in cooperation with S1, will provide support and guidance on best practices. The UCC will maintain and administer the vendor contract for this project.

For a full list of S1 privacy terms and conditions please visit https://www.sentinelone.com/legal/

MDR Project: Policy

This project will provide LGE’s with access to the SentinelOne Endpoint Protection Platform with the following capabilities:

- Singularity Complete - Endpoint Detection & Response (EDR)
    - 90-Day Retention of all EDR data
- Managed Detection & Response (MDR)
- Singularity Ranger Insights - Vulnerability Management
- 24/7/365 Technical Support
- Technical Account Manager (TAM)
- Limited access to Digital Forensics and Incident Response (DFIR)

The LGE can utilize this resource after they have been onboarded and approved for deployment by the UCC team, and continuing throughout the project period. The MDR Project should be used continuously after deployment as a primary Endpoint Protection solution. The S1 platform can only be deployed to devices that are owned and operated by the LGE.

The Vigilance MDR service will provide the LGE with a team of expert analysts from S1 who will monitor your endpoints and respond to alerts 24/7. This team will take various prevention and remediation actions on the LGE endpoints, in coordination with, and as defined by the LGE.

MDR Onboarding SOP

Onboarding will generally follow this predefined process:

- Phase 1: Initial contact related to the MDR project between the UCC and the LGE
    - An introductory meeting between UCC and the LGE is arranged
        - This meeting will outline the project details and provide the LGE with instructions on how to perform a limited deployment
- Phase 2: MOU and other details are collected
    - LGE returns a signed copy of this MOU to UCC
    - LGE completes an onboarding survey
    - LGE provides escalation contact information to S1
- Phase 3: During this phase, the LGE will perform a limited deployment allowing for the discovery of interoperability issues and to perform fine tuning of the environment
    - A follow up meeting between UCC, the LGE, and S1 will take place after adequate testing has been performed
        - This meeting will serve as a check in point to review the test deployment progress, policies, interoperability exclusions, deployment of sensors, and other best practices, specifically LGEs should never disable Agent Anti Tamper.
- Phase 4: Full deployment
    - LGE will continue to deploy sensors across the entire environment.

SOP for requesting use the S1 DFIR Retainer

In the event of a cybersecurity incident indicating the need for the use of Digital Forensics and Incident Response (DFIR) capabilities from S1, the LGE can initiate a DFIR initial evaluation request by contacting DFIR@sentinelone.com. The State contract includes a limited yearly bucket of available DFIR hours. Due to the limited nature of the DFIR retainer, these services should only be engaged when dealing with a serious incident. After the initial triage is complete the LGE, DFIR team, and UCC will coordinate in order to determine the necessity of continuing the expenditure of the retainer hours.

Prior to an LGE engaging the DFIR team and expending the retainer, the LGE is strongly encouraged to contact their Cybersecurity Insurance provider, if they have one, to inquire about similar services that will be funded through their plan. LGE's should contact their insurance providers before an incident to better understand the resources available to them. LGE's can purchase their own block of DFIR hours directly from S1 if desired.

SOP for acquiring additional, non-grant funded capabilities

S1 has agreed to allow LGE's to purchase additional capabilities that are available in the S1 platform directly, including DFIR retainer hours. UCC will not fund any capabilities beyond what has been described. All additional services must be paid for and contracted between the LGE and the vendor directly.

Technical Support SOP

Technical support is available 24x7x365. All support issues should be raised by first creating a ticket through the web portal or by calling the support number listed below.

https://community.sentinelone.com/
Phone Support: 1-855-868-3733

Issue Severity levels are defined as follows:

- Severity 1 - Critical Business Impact, affecting critical Business Unit or site-wide issue.
    - Ex. Solution is inoperative, intermittently operative, unavailable or significantly impaired. Compromise of system operability with multiple system failures, compromise of data integrity, or loss or corruption of data, complete failure of the system.
- Severity 2 - High Business Impact; Multiple machines affected via a critical service degradation.
- Severity 3 - Business is impacted, but your organization can function properly.
- Severity 4 - No Business impact, low priority issue or request for a feature.

For Severity 1 events, LGE's are encouraged to contact the Technical Account Manager for support in escalating the ticket, after ticket creation.

Escalations SOP

The Escalations process will be determined between the LGE and the S1 team during the onboarding process. This will include providing escalation contacts to S1. It is the responsibility of the LGE to maintain this contact list. It is expected that this list will be continually maintained and updated as appropriate, without undue delay.

The UCC SOC will serve as an emergency backup point of contact for your organization at your request, in the event that your team is unable to be contacted during an escalation event. In the event of an escalation call reaching the UCC SOC, the SOC will continue efforts to contact your organization using out of band channels, possibly including through emergency dispatch services. Please select an option from the list below by checking and initialing the appropriate section.

☒ _____I **would like** the UCC SOC to act as an emergency back up contact for S1 Vigilance escalations.

☐ _____I **decline** the offer to have the UCC SOC act as an emergency back up escalation contact for my organization.

Threat Hunting SOP

UCC will periodically perform threat hunting using IOCs from a multitude of sources. The UCC will be performing these activities across the entire S1 environment. If a correlation between an IOC and your environment is found, UCC will contact you with details. Any IOCs generated during threat hunting will have any identifying information removed, so they can be shared with the wider cybersecurity audience as appropriate.

STAR Rules are a limited resource and are intended to be used for global threat hunting. LGEs should leverage Saved Queries for threat hunting within individual LGE accounts. Should an LGE desire that a STAR rule be created, this can be requested by contacting the UCC. This will afford increased protection to all participating LGEs.

MDR Project: User Procedure Requirements and Maintenance

By signing this agreement each participating LGE agrees to deploy and maintain the MDR platform within their environment and follow any SOPs outlined in this MOU. Agent deployment and maintenance, user accounts and role assignments, and administrative console maintenance are the responsibility of the LGE. S1 support staff and UCC staff are available to assist and provide best practices for this process. In the event that console access is lost and the LGE has no administrator access, this can be restored by working with the UCC to establish new accounts.

The purpose of these procedure requirements is to ensure LGEs' systems are being effectively protected by the MDR service and that the product is being leveraged to its fullest potential.

MDR Project: Oversight

Oversight of the MDR Project is administered through the UCC, which is directed by the Utah State Chief Information Security Officer (CISO). The UCC oversees the use and/or licensing of the MDR Project services and will enforce all requirements of this MOU. Each LGE participating in the use of the MDR Project is required to provide a representative, through whom the UCC will coordinate provisioning of the service. Any issues affecting policy, recommendation, and/or subsequent change that alter the purpose of the MDR Project will be implemented at the discretion of the UCC.

Project 2 - Vulnerability Management Project

This project will utilize the same agent installed from the MDR project to help identify and prioritize an LGE's most critical applications and operating systems vulnerabilities for both workstations and servers. Participation in this project is included in the MDR Project.

Project 3 - Security Professional Training

This project will provide LGE's with access to instructor-led training geared towards those with an Information Technology background. The UCC will determine what courses are offered, taking into consideration input from LGEs. The UCC will communicate these opportunities to the LGE via Email. The training will increase participants' knowledge on security topics and allow for them to use and apply to their organization to help them secure their environment. Project 3 will be funded initially through State and Local Cybersecurity Grant Program (SLCGP) funds with a period of performance lasting from 10/31/2023 through 12/31/2027. The UCC will maintain and administer the vendor contracts for this project.

LGE's IT personnel should participate in this training to help increase their cybersecurity knowledge and apply it to their own organization's environment to help improve the security posture of the organization. Should the offered training include an opportunity to test and become certified, it is expected that the participant will schedule and take the exam.

Participation in these trainings is limited. The UCC will use multiple factors to determine which applicants are selected for the training. These factors will include: timeliness of the application, position and role of the applicant at the LGE, previous experience of the applicant, and number of applicants from the same LGE.

Requirements for necessary equipment will be communicated when an applicant is selected for participation in the training program. Training formats may be offered virtually or in-person at select locations. Locations will be communicated upon training announcements. The UCC will not provide funds to cover any travel, accommodations, or equipment required for participation.

If an applicant is selected for the training program but is unable to attend, the UCC staff must be notified. If insufficient time is given to find a replacement for the participant, the LGE may be held at a lower priority when being considered for future training opportunities.

Project 4 - Security Awareness Training Program

Participation in this program places no financial or contractual obligation, beyond what is defined in this MOU, on the LGE. This service is being provided at no cost for the project period of 10/01/2023 through 10/05/2027. This MOU and Security Awareness service will automatically terminate at the end of that period (10/05/2027). Should the LGE wish to discontinue use of this Security Awareness Training Program and terminate the MOU sooner than the defined end date of the project, the authorizing official of the LGE will need to notify the UCC in writing three weeks prior to termination.

Each LGE will have their own account that is visible only to their staff and UCC Global Administrators. Each LGE can build and configure their program however best suits their needs. LGEs will have full administrative rights to their accounts.

UCC staff will be the only entity assigned Global Administrator access. UCC will not perform any actions inside of a LGE account without the LGE expressly requesting the action be taken. UCC, in cooperation with KB4, will provide support and guidance on best practices. The UCC will maintain and administer the vendor contract for this program.

Security Awareness Training Program: Policy

This project will provide LGE's with access to the KB4 Security Awareness Training Platform with the following capabilities:

- Security Awareness Training
    - Platinum Subscription level with Compliance Plus Add-On
- Phishing Campaigns
- USB Security Test
- Generate and Schedule Reports

The LGE can use this resource after they have been onboarded and approved for deployment by the UCC team, and continuing throughout the project period. The Security Awareness Training Program should be used periodically throughout the year, as each LGE sees fit, to train and provide awareness to their employees on cybersecurity topics. Phishing campaigns should also be conducted in this same manner to provide employees with real world examples of this common type of attack while teaching them how to be aware and defend against it.

Security Awareness Training Program Onboarding SOP

- LGE contacts UCC
- LGE signs and returns MOU
- UCC creates account for LGE and provides initial administrator access
    - LGE operates and manages their own environment going forward throughout the project period

SOP for acquiring additional, non-grant funded capabilities

Add-ons, upgrades, and additional capabilities beyond what is provided in the policy above are not available in the KB4 platform.

Technical Support SOP

Technical support issues should be addressed by first consulting the KB4 knowledge base.If you can't find the information you need in KB4's knowledge base or you need assistance using their products, you can contact KB4's support team by submitting a support request through the web portal or by calling the number below.

Knowledge Base: https://support.knowbe4.com/hc/en-us
Submit a request: https://support.knowbe4.com/hc/en-us/requests/new
Phone Suppor+t:1 855-815-9494, available weekdays from 4am - 7pm

UCC Security Message Campaign

The UCC Security Message will be distributed periodically throughout the year and include a monthly short newsletter-style message promoting cybersecurity awareness and quarterly training campaigns to raise awareness of common cybersecurity topics and attacks. The message and training campaign will be sent to all users of participating LGEs.

☒ _____**I would like to participate in the UCC's Security Message campaigns**.

Should your LGE decide to discontinue participation in this service simply contact the UCC at cybercenter@utah.gov to cancel.

UCC Email Phishing Campaign

The UCC Email Phishing Campaign will be conducted periodically throughout the year and provide a method of testing user awareness. The UCC will coordinate with the LGE administrators in advance so they are aware of the upcoming campaign. The phishing emails will be sent to all users of participating LGEs.

☒ _____**I would like to participate in the UCC's Email Phishing campaigns**.

Should your LGE decide to discontinue participation in this service simply contact the UCC at cybercenter@utah.gov to cancel.

Security Awareness Training Program: User Procedure Requirements and Maintenance

LGEs are responsible for provisioning their user accounts in the KB4 system. Technical support provided by KB4 is available to assist with user integration issues. User accounts, role assignments, and administrative console maintenance are the responsibility of the LGE. Training and phishing campaigns are performed and managed by the LGE except for the UCC Security Message Campaign and the UCC Email Phishing Campaign outlined above. In the event that console access is lost and the LGE has no administrator access, this can be restored by working with the UCC to establish new accounts.

Security Awareness Training Program: Oversight

Oversight of the Security Awareness Training Program is administered through the UCC, which is directed by the Utah State CISO. The UCC oversees the use and/or licensing of the KB4 platform services and will enforce all requirements of this MOU. Each LGE participating in the use of the Security Awareness Training Program is required to provide a representative, through whom the UCC will coordinate provisioning of the service. Any issues affecting policy, recommendation, and/or subsequent change that alter the purpose of the Security Awareness Training Program will be implemented at the discretion of the UCC.

Section 5: Responsibility for Compliance

Failure to operate within the bounds outlined within this MOU, or actions taken by the LGE that are determined to be detrimental to the project's success could result in the LGE being removed from participation in any of the statewide projects.

The state is not responsible for damages or disruptions to services that result from actions taken by LGE's within their environment.

Section 6: Updates to the MOU

The UCC has the authority to update and modify this MOU for any of the current projects or to add future projects. In the event that a proposed change or additional statewide project is added which alters the capability or changes the purpose of the statewide projects, a new signature page verifying the understanding of changes will be required. As the MOU is updated, a new copy will be made available to the participating LGEs.

Section 7: Signatures & Agreements

The State of Utah Cybersecurity Planning Committee created a statewide cybersecurity plan which outlined specific cybersecurity initiatives, programs, and objectives aimed at improving local government cyber maturity. It contains projects targeted at remediating deficiencies identified through multiple assessments and audit efforts. These projects will be funded through the use of SLCGP funds and will provide services for 4 years. The estimated value of these services is $10,564,058, which will be funded through the use of the grant award plus the required matching funds.

The projects are:

Project Name	Project Description
Managed Detection and Response Project	Provide licenses for a whole-of-state implementation of a managed detection and response (MDR) solution.
Vulnerability Management	Provide licenses for a whole-of-state implementation of a vulnerability management solution.
Security Professional Training	Organize and provide access to professional cybersecurity training.
Security Awareness Training Program	Provide access to a security awareness training platform for government employees.

I understand that by participating in any of these statewide programs I am consenting to the State of Utah retaining and using grant funds, awarded through the SLCGP in order to provide our organization with cybersecurity hardware, software, and/or services in lieu of direct funds, for the listed projects.

By signing this document I attest that I am either the authorizing official, or have been designated by the authorizing official of our organization to enter this agreement.

Our organization wishes to participate in Utah Statewide SLCGP Projects and agrees to the terms of this MOU.

Date	Print Name
Signatory's Title	Signature

Fields below this line are to be filled out by the Utah Cyber Center. Do not edit these fields.

The Utah Cyber Center agrees to the terms of this MOU, and will fulfill the responsibilities outlined within this agreement.

Date	Phil Bates Print Name
CISO, DTS Signatory's Title	Signature