INSTITUTE *of* Museum and Library SERVICES

Museums Empowered

Sample Application ME-249264-OMS-21
Project Category: Digital Technology

Children's Museum of Indianapolis

Amount awarded by IMLS:	$250,000
Amount of cost share:	$389,025

The project description can be viewed in the IMLS Awarded Grants Search:
https://www.imls.gov/grants/awarded/me-249264-oms-21

Attached are the following components excerpted from the original application.

- Narrative
- Schedule of Completion

When preparing an application for the next deadline, be sure to follow the instructions in the current Notice of Funding Opportunity for the grant program and project category to which you are applying.

"SAFEGUARDING MUSEUM ASSETS BY REVAMPING TECHNOLOGY & STAFF CAPACITIES"

PROPOSAL NARRATIVE

1. PROJECT JUSTIFICATION

The Children's Museum of Indianapolis (Museum) requests a grant of $250,000 from the Institute of Museum and Library Services' Museums Empowered program in support of the proposed "Safeguarding Museum Assets by Revamping Technology and Staff capacities" (SMARTS) project, which will enhance the Museum's capacities to prepare for and respond to new and evolving cybersecurity threats, including those related to the COVID-19 public health emergency. The project will generate important systemic change within the Museum, improving security infrastructure and practices across departments. In doing so, IMLS funding will support the Museum's ability to continue serving its public safely and securely through innovative new virtual programs launched at the outset of the pandemic.

The Museum is the largest children's museum in the world and has an annual visitation of more than 1.3 million, ideally positioning it to test innovations in virtual and on-site programs and share best practices throughout the museum field. The Museum's 489,000 square-foot, 5-level facility sits on 29 acres and houses 13 permanent exhibits and 4 temporary galleries that draw on a collection of more than 130,000 objects. The Museum is also home to a 7.5-acre health and fitness experience, a professional children's theatre, and the nation's only full-service public library inside a museum. These exceptional facilities, coupled with the Museum's 327 professional staff and a volunteer base of more than 1,000 enable the Museum to fulfill its mission of *creating extraordinary learning experiences across the arts, sciences, and humanities that have the power to transform the lives of children and families*. The Museum is committed to continuing innovations started in 2020 to provide engaging virtual programming for visitors and students and is enthusiastic about sharing best practices and lessons learned through these efforts with the broader Museum field. An important aspect of these learnings will be strategies developed to update Museum staff capacities and IT infrastructure to protect against the vulnerabilities associated with its rapidly expanding virtual footprint—areas where the project will provide funding and technical support to help the Museum fully achieve its goals.

Needs to be Addressed:

<u>Supporting a Virtual Pivot:</u> The COVID-19 public health emergency and a corresponding Museum closure of nearly four months highlighted the criticality of responding to the needs of visitors, donors, and staff in new ways not identified previously. The Museum pivoted rapidly to offer engaging new, virtual experiences for children and families, launching its new flagship virtual program, *Museum at Home*, within days of its closure. *Museum at Home* brings the Museum's collections and programs directly to the homes of children and families across the U.S. and the world, allowing them to take virtual exhibit tours, chat with experts, learn to curate their own collections, and conduct guided science experiments. To-date, *Museum at Home* has generated 11.2 million media impressions and has garnered critical acclaim from CNN[1], *USA Today*[2], the *Los Angeles Times*[3], and Forbes[4] and was named the MVP museum virtual education campaign by the MCN Blog[5] (footnotes in Supporting Document 1). Over the past eight months, the Museum's virtual offerings have grown steadily in response to audience demand, hosting virtual donor events, creating virtual school field trip programs, and hosting free virtual arts and cultural programs—all in an effort to enhance public access to the Museum's extraordinary collections and programming. This significant new demand for virtual learning experiences provides enormous opportunity to expand the Museum's impact beyond its physical boundaries, generating engagements across the country and beyond.

<u>Social Media Risks:</u> The platforms the Museum has utilized to expand its virtual offerings are vulnerable to intrusions, both due to lack of staff users' cybersecurity knowledge as well as to vulnerabilities in the coding of the platforms themselves. Expanded use of video conferencing software such as Zoom, which the Museum uses to host virtual events with hundreds of participants, has created new risks. Zoom is subject to intrusions caused by lax user security—a phenomenon so widespread it was dubbed "Zoom Bombing"[6]—but is also vulnerable to malware due to its software configuration.[7] The growing dependence of the Museum and other institutions on social media like Facebook, Instagram, and Twitter as a means of facilitating audience engagement is also not without its risks. In 2016, cybersecurity researchers found that 1 in 8 U.S. organizations had experienced a security breach from a social media-directed cyberattack.[8] As social media usage spiked to record highs in 2020 amid stay at home orders[9]—a factor that made the successes of *Museum at Home* possible—

cybercriminals followed suite. Reports of social media-based phishing scams are on the rise,[10] as are malicious hacks of social media accounts, including a highly publicized Twitter hack in July that took control of notable profiles including Apple, Bill Gates and former President Barack Obama, among others.[11]

Data Security Risks: By April 2020, less than a month into the Museum's four-month closure, the FBI's Cyber Division had reported a spike of 300-400% in the number of cybersecurity complaints received daily.[12] A global poll of IT professionals in April found that 71% reported an increase in security threats or attacks since the beginning of the COVID-19 outbreak.[13] The Museum was no exception. The Museum's Information and Infrastructure Technologies (IIT) Team observed a 260% spike in attempted malicious intrusions and phishing scams in March compared to the first two months of 2020. Were these intrusions to result in a breach of the Museum's visitor or donor data, the results could be devastating. Based on the average $150 cost per record stolen, as pinpointed in an IBM Security study,[14] a massive breach, for instance, of the Museum's customer relationship management (CRM) or e-commerce systems could cost up to $118 million—a figure that does not take into account the difficult-to-quantify costs of damage to the Museum's reputation and brand that would result from such a breach.

Challenges of Remote Work: These risks are compounded by a rapid pivot to remote working. Following the Museum's closure in March, all but the most essential on-site personnel (more than 400 at the time) transitioned to remote work. Though the Museum has since reopened, more than half of its staff continue to work from home to allow for social distancing. Remote work carries increased risks for data breaches. The FBI's Cyber Division attributed this year's jump in cybersecurity complaints to the rapid rise in telework.[15] Remote work arrangements can also make security breaches more difficult to resolve, with 76% of organizations in a recent survey saying that remote work would increase the time it took to identify and contain a data breach.[16]

Infrastructure Strain: The high rates of staff working remotely, combined with ever-increasing numbers of visitors accessing the Museum's website and other virtual assets, has placed a significant burden on the Museum's aging IT infrastructure. The Museum's servers are nearing capacity, and more than 25 of the Museum's 58 network switches are beyond the manufacturer's end-of-life date, putting them out of the service period for updates and support and making them more susceptible to intrusions. Three of the Museum's servers will reach end-of-life date prior to the start of the proposed SMARTS project. Investments in the aging infrastructure that supports the Museum's expanded virtual capabilities and ensures data security are critical to the Museum's long-term viability.

Staff Capacities: Multiple and simultaneous investments in staff cybersecurity capacities are also necessary to safeguard the Museum, its visitors and donors from attempted intrusions. A recent IBM Security analysis of large businesses found they experienced 3.2 data breaches per year on average due to an employee or contractor, with the vast majority (60%) being caused by human error—either inadvertently or through negligence.[17] The staff who interface with the Museum's data, servers, and social media accounts remain one of the most important factors in keeping the Museum and its end-users safe, pointing to the need for institution-wide capacity building. A white paper, "Staying Safe: Cybersecurity in Modern Museums," which was presented at the 2017 Museums and the Web conference, put it simply: "*Staff members are your human firewall. In order to function in this critical role they need awareness training so they can spot a suspicious email or unusual computer behavior. Staff should know how to report such an event and how to stop an infection from spreading*."[18]

Studies, Plans & Best Practices:

IIT Disaster Recovery Plan: In recognition of these pressing needs, the Museum created an IIT Disaster Recovery Plan (Supporting Document 2) in April 2020 to ensure information system uptime, data integrity and availability, and business continuity in the case of an emergency or systems failure. The Plan included a risk analysis which identified the most likely IIT disasters for which the Museum should prepare, including acts of terrorism or sabotage against the Museum's IIT systems as "likely" events (scoring a 4 on a 5-point scale of likelihood), with the potential to cause "severe" damage (scoring a 5 on a 5-point scale of impact). The Plan is to be implemented in three phases:

1) Migrate business-critical systems, including the Museum's CRM, collections management (KE-Emu), and financial systems to a Disaster Recovery as a Service (DRaaS) provider, a cloud computing backup service model using cloud and/or co-location (local cloud) resources to protect against data disruptions;
2) Migrate applications and business support systems to the cloud; and
3) Introduce off-site physical and virtual back-ups. Phase 1 will be implemented by the end of 2020, while Phases 2 and 3 will be supported in part by the SMARTS project.

IIT Hardware and Software Asset Management Policy: The Museum's practices for replacement, rotation, and access to IIT assets, as outlined in its Asset Management Policy (Supporting Document 3), also adhere to industry standards and outline procedures for acquiring, deploying, monitoring and maintaining IT assets, including inventory, security, and surveillance practices. Equipment replacement schedules account for depreciation and manufacturers' end-of-life dates**.**

Best Practices in the Museum Field: The above-mentioned plans are just part of the Museum's cybersecurity efforts. The "Cybersecurity in Modern Museums" white paper specifies that *"An effective cybersecurity approach should include network firewalls and gateways, anti-malware, user access management and authentication controls, backup management, business continuity and disaster recovery planning, patch management, and software updates. These will be bolstered by staff education."*[19] The Museum currently employs all of these methods and will further bolster the critical areas of staff education, backup management and software updates (via deployment of new, in-service servers) under the SMARTS project.

Cybersecurity Audit and Industry Standards: The Museum is in the process of conducting a Cybersecurity Audit that will provide detailed guidance on specific vulnerabilities related to IIT practices and staff capacities. The audit will be conducted at the end of 2020 and will utilize a collective methodology based on industry standards from the National Institute of Science and Technology (NIST), the Open Source Security Testing Methodology Manual (OSSTMM), the International Council of Electronic Commerce, the Payment Card Industry Security Standards Council, Offensive Security, the Penetration Testing Execution Standard (PTES), and the Open Web Application Security Project (OWASP). Finally, the Museum's staff training policies also forward best practices in the industry, such as those expounded by the SANS Institute for Cybersecurity training.

Beneficiaries:

Museum audiences: Enhanced cybersecurity practices and infrastructure at the Museum will ultimately benefit all of the Museum's 1.3 million annual visitors by ensuring the safety of their data. The Museum's visitors are highly diverse, with 20% identifying as BIPOC, compared to the national average of 9%, as reported by the American Alliance of Museums (AAM)[20]. Additionally, 21% of Museum visitors are low-income families who benefit from free or reduced-price admissions. In particular, the 2,179,000 contacts for whom the Museum maintains personal and financial data in its CRM and e-commerce systems, will specifically benefit from the project. These include visitors, donors, vendors, board members, and beneficiaries of the Museum's community programs. Moreover, the millions of users globally of the Museum's virtual *Museum at Home* content and virtual school field trips will benefit from increased website response time, resulting in an improved virtual experience.

Museum Staff: All Museum staff will benefit, not only from increased cybersecurity knowledge, but also from new abilities to continue working in the case of a network outage or other disruption, as well as from enhanced safeguards of their personal and financial data, which is also maintained by the Museum as part of its personnel and payroll systems.

The Museum Field: Lessons learned from the project will be made available for the benefit of other arts and cultural institutions. The project will initially focus on sharing cybersecurity learnings and resources—including relevant findings from the cybersecurity audit—with institutions with which the Museum regularly shares data, such as the InfoZone branch of the Indianapolis Public Library located inside the Museum, and the 11 Indiana arts and cultural institutions that partner on its Access Pass program. (Because Access Pass provides discounted $2 admissions to low-income Indiana families at all partner institutions through use of a single membership card, cardholder data must necessarily be shared among participating institutions. For a list of Access Pass partners, see Supporting Document 4.) By the end of the project, lessons learned will be disseminated on a wider scale through museum associations and networks, as outlined below under "Results Dissemination."

Advancing the Museum's Strategic Plan:

The SMARTS project will advance the Resource Development goal of the Museum's Strategic Plan for 2019-2021. The "Data Security" objective under this goal calls on the museum to *"maintain technology-based platforms that further the Museum's ability to manage earned and contributed revenue in a secure data environment."* Metrics for this objective include:

- an uptime of 99.96% for all financial and fundraising systems, and
- positive annual assessments and certifications of data security practices.

The project will contribute to the plan's Content Development & Delivery goal, and its "Interactive Technology" objective by:

- increasing website response time for online visitors accessing new virtual content, and
- providing secure, redundant back-ups of virtual assets to decrease or eliminate downtime in the event of a disruption.

Alignment with Museums Empowered goals and categories:
The SMARTS project falls within the Digital Technology category of the Museums Empowered initiative, as it seeks to increase the capacities of Museum staff to understand emerging cybersecurity threats and safeguards, generating systemic change by prompting staff from across the Museum to view cybersecurity as central to their roles and responsibilities as well as to the overall success of the institution. This will contribute to the Museums Empowered goals by strengthening the Museum's ability to serve its public—including visitors, donors, community initiatives participants, board members and staff—through enhanced data safeguards and improved ability to continue uninterrupted service provision in the face of network disruptions.

2. PROJECT WORK PLAN

The planned activities directly correspond to the project's intended results (see ""Project Results," below) in that they will decrease vulnerability to cyberattacks and network disruptions through improved IT infrastructure (Result 1 / Activity Grouping 1) and enhanced staff capacities (Result 2 / Activity Grouping 2), while also mitigating the effects that a successful cyberattack or prolonged network disruption would have on the Museum and its audiences and increasing server response time (Result 3 / Activity Grouping 3). Activity Grouping 4 describes planned evaluation activities. Further detail on the timing and sequencing of project activities is included in the Schedule of Completion, attached.

(1) Activities Corresponding to Result 1 – Improved IT Infrastructure:

- Activity 1.1: Equipment Procurement – The Museum's IIT Department will procure at least 3 new servers and 25 new switches to replace those that are farthest out of service or beyond end-of-life dates. Procurement will be conducted in line with Federal and Museum guidelines.
- Activity 1.2: Equipment Installation – New servers and switches procured in Activity 1.1 will be installed and configured either by the vendor or by a third-party installer overseen by the Museum's IIT Department. Equipment will fully installed within four months of the project start date.
- Activity 1.3: Software Updates and Maintenance – The new equipment will be kept up to date with the latest security updates and bug fix patches, ensuring dependable function and providing protection against malicious intrusions.

(2) Activities Corresponding to Result 2 – Enhanced Staff Cybersecurity Capacities:

- Activity 2.1: Recruit a Cybersecurity Expert – The Museum will procure through a competitive selection process a cybersecurity expert to provide guidance on staff cybersecurity capacity building development under the project (Activities 2.2 and 2.3, below). The selected expert will have proven experience successfully working with staff who have a varying degree of technical knowledge in order to address and mitigate specific cybersecurity vulnerabilities identified in an institution-wide Cybersecurity Audit conducted at the end of 2020 (Activity 4.1).
- Activity 2.2: Museum-wide Staff Cybersecurity Training – The IIT Team will develop a Staff Cybersecurity Training 2.0 webinar to follow-up to an initial training rolled out in 2020, which includes practical tabletop exercises and covers topics such as phishing and threat mitigation. The 2.0 training will be updated based on staff feedback from the first training and will include new content developed with the cybersecurity expert to address vulnerabilities identified in the baseline Cybersecurity Audit. The training webinar will be mandatory for all staff to complete by mid-2022.
- Activity 2.3: Targeted Cybersecurity Training/Coaching – The cybersecurity expert and IIT Team will develop a series of targeted cybersecurity trainings or coaching sessions for specific staff or departments identified as vulnerable in the Cybersecurity Audit completed at the end of 2020. The trainings will focus on specific areas of need including phishing awareness and detection, prevention, and other specific vulnerabilities identified in the Cybersecurity Audit.

(3) Activities Corresponding to Result 3 – Enhanced Mitigation and Response Time:

- Activity 3.1: Off-site and Cloud Back-ups – The project will support Phase 3 of the Museum's IT Disaster Recovery Plan, introducing physical and cloud-based data back-ups off-site through a platform like Veeam.
- Activity 3.2: Bridging On-Site and Cloud Servers – The IIT Team will bridge internal switches and servers (both existing and new) to cloud infrastructure in order to increase website response time, improving the experience for on-site visitors (e.g. via advance ticket booking) and online visitors participating in virtual programs, as well as enhancing productivity and security of the Museum's remote workforce and reducing the Museum's carbon footprint.

(4) Evaluation Activities:

- Activity 4.1 (pre-project activity): Baseline Cybersecurity Audit – Prior to the start of the project, at the end of 2020, the

Museum will conduct a cybersecurity audit with an external cyber risk, compliance, audit and penetration testing firm, Mako Group. (Because it will take place prior to the start of the grant period, this audit is not included in the grant budget nor in the Museum's matching funds toward the project.) The results of this audit will form the baseline for the SMARTS project and will provide data on key areas where cybersecurity improvements are needed—particularly in terms of staff capacities. (A Statement of Work for this audit is included in Supporting Document 5.)

- Activity 4.2: Mid-Term Cybersecurity Audit – In the second year of the project (2022), the Museum will conduct a mid-term cybersecurity audit to track progress made toward project results by assessing the degree to which Activities 1-3 have improved the Museum's cybersecurity to-date and pinpointing areas of further improvement. This data will help the Project Team make adjustments as needed to ensure intended results are achieved.
- Activity 4.3: (post-project activity): End-line Cybersecurity Audit – Following project conclusion in 2024, but prior to submission of the final project report, the Museum will conduct an end-line cybersecurity audit to assess the degree to which project activities improved the Museum's overall cybersecurity as compared to the baseline and end-line audits. These results will be included in the final project report. (Because this activity will take place after the end of the grant period, this audit is not included in the grant budget nor in the Museum's matching funds toward the project.)

Risk Assessment and Mitigation:

Cybersecurity Risks: The project is designed to mitigate cybersecurity risks to the Museum's operations and data. The IT Disaster Recovery Plan identified electrical power failure and loss of communications network services as the most likely disasters that the Museum would face (both were ranked as 5/5 on a probability scale where 5 represented an almost certain possibility). The risks that would have the most impact on the organization included loss of communications network services, acts of sabotage, and acts of terrorism (all were ranked as 5/5 on an impact scale where 5 represented the most severe impact). All the risks that would be most likely and impactful will be addressed through the proposed project's activities.

COVID-19: Disruptions to Museum visitation and operations as a result of the ongoing COVID-19 public health emergency will continue to pose a risk to all Museum projects until a vaccine or effective treatment is developed, according to data from internal visitor surveys and consultations with the Museum's scientific and medical advisory panel. The Museum will mitigate these risks by consulting with its Board and advisors regularly to respond to the rapidly changing situation and to implement guidance from local, state, and national health officials effectively. Financially, the Museum's endowment provides some buffer to allow for continued Museum operations despite significant losses in earned revenue.

Project Team – Museum Staff:

- ***Kathy Mathena, Chief Information Officer,*** will serve as the Project Director, providing oversight of the Project Team and consultants. Ms. Mathena has more than 12 years' experience in information systems management and prior to starting at the Museum in 2019 served as the Executive Director of Clinical Information Systems for Indiana University Health. She will oversee Project Team meetings and she will serve as the project liaison with the Museum's Executive Team and Board, building institution-wide ownership of the project specifically and efforts to enhance cybersecurity more broadly.
- ***Yvel Guelcé, Director of Infrastructure Technology,*** will be responsible for implementation of activities related to Results 1 and 3, will oversee staff working on activities related to Result 2, and will jointly manage cybersecurity audit and evaluation activities with Ms. Mathena. Mr. Guelcé has 35 years' professional experience in the IT field, and since 2007 has focused on technology deployment in a museum context—first at the Indianapolis Museum of Art (Newfields) and currently at The Children's Museum—winning back-to-back AAM Media & Technology Muse awards for his work.
- ***Andrew Innes, IT Infrastructure and HelpDesk Manager,*** will be responsible for staff cybersecurity training activities, working alongside an external cybersecurity expert. Mr. Innes has 14 years of experience in IT support and network administration. He holds a degree in Electrical Engineering Technology from Northern Alberta Institute of Technology.
- ***Marc Davies, IT HelpDesk Analyst,*** will support Mr. Innes in staff cybersecurity training and will support Museum staff in troubleshooting issues that may arise during installation of new IT infrastructure (Result 1) or cloud migration (Result 3). Mr. Davies is a Microsoft Certified Technology Specialist holding a B.S. in IT Security from Western Governors University.
- ***Mike Copple, Business Intelligence Data Architect,*** will be involved in Result 2 and 3 activities as they pertain to the safeguarding of institutional data and migration of CRM records. Mr. Copple has 10 years' experience in data analysis and programming and is an expert in SQL, SSIS, SAS, and STATA. He has an M.A. in Economics from Indiana University.

- ***Jonathon Bailey, Audio-Visual Services Manager,*** will assist with Result 1 activities related to the installation of new servers and switches supporting audio-visual elements of exhibitions and virtual programs. Mr. Bailey has nearly a decade of experience in film and video production. He holds a degree in Film and Video Studies from Purdue University.

Project Team – Consultants & Contractors:

- ***External Cybersecurity Auditor:*** The Museum will work with (an) external cybersecurity auditor(s) to conduct baseline, mid-term, and end-line cybersecurity audits during the project. The Museum's internal financial and procurement controls require that external consultancy contracts over $10,000 be competitively procured. The Museum has already procured Mako Group to conduct the baseline audit in 2020 (see Supporting Document 5). Mako and similar cybersecurity firms that follow rigorous, industry-standard cybersecurity audit and penetration testing methods, as outlined under "Studies, Plans, and Best Practices," above, will be invited to submit a proposal. The Museum will ensure consistency in its RFPs to ensure the cybersecurity capacities being assessed remain consistent between the baseline, mid-term, and end-line audits.
- ***External Cybersecurity Consultant:*** The Museum will recruit an external cybersecurity expert consultant to lead development of staff cybersecurity capacities Result 2 activities. An RFP will be developed at the start of the project, with specific areas of expertise required to be informed by the results of the baseline Cybersecurity Audit conducted at the end of 2020. The selected expert will have demonstrated expertise in risk management and security services with a proven record in effective cybersecurity training strategies and techniques, including the importance of building a culture of security awareness and ownership at every level of the organization. The selected expert would promote an environment that balances personal responsibility in keeping the Museum secure with a commonsense approach.

Financial and Other Resources:

In addition to salaries and benefits for IIT staff time spent on the project, the project budget will also support enhancements to the security of the Museum's aging IT infrastructure through the purchase of 3 servers and 25 network switches. The project will fund a cybersecurity expert to assist with capacity building and a cybersecurity audit firm to conduct a mid-term audit to assess progress against project results and to flag remaining vulnerabilities. The SMARTS project will be informed by data from a baseline cybersecurity audit in 2020, which will be funded separately by the Museum. A final cybersecurity audit to take place after the end of the project but prior to final reporting will also be covered by the Museum. Other resources that will support the SMARTS project but which are not included in the budget include time of the Museum's Executive Team (with the exception of the CIO, who is the project director) and Board, and time of staff spent in project-related trainings and support sessions.

Tracking Progress Toward Results:

The baseline, mid-term and end-line cybersecurity audits described above ("Activity Description") and below ("Data Collection") will serve as the key instruments for tracking project progress toward intended results. Audit findings will be reviewed by the Project Team to identify needed adjustments in order to ensure successful achievement of project results. Additionally, the Project Team will meet regularly (at least monthly) to assess progress against the Schedule of Completion and project budget.

Results Dissemination:

Results from cybersecurity audits will be shared beyond the Project Team, including with the Museum's Executive Team, Board, Associate Vice Presidents, and Directors, in order to promote institution-wide ownership of the project and awareness of the importance of cybersecurity improvements across all Museum departments. Lessons learned and materials, including the Cybersecurity Training 2.0, will be made available to other arts and cultural institutions, including the InfoZone branch of the Indianapolis Public Library and 11 Access Pass partner institutions. Lessons learned and materials will also be disseminated to the larger museum field through presentations, webinars and whitepapers for the annual conferences of the MCN and/or MuseWeb (MW).

3. PROJECT RESULTS

Intended Results:

The project will take a three-pronged approach to address institutional cybersecurity needs and gaps. Results 1 and 2 focus on IT infrastructure and staff capacities, respectively, and are preventative in nature, aiming to decrease the likelihood of a cybersecurity event (e.g. phishing scam, hack, etc.) that results in a breach of institutional data or loss of operational functionality. Result 3 focuses on mitigation of potential cybersecurity events and will support implementation of Phases 2 and 3 of the Museum's Disaster Recovery Plan, which will decrease or eliminate down-time resulting from a cybersecurity event while also proactively improving the experiences of visitors and staff who interface with the Museum's servers (e.g. via the Museum website, virtual content, or remote working).

- ***Result 1:*** Decrease institutional vulnerability to cyberattacks and increase the security of visitor, donor, staff, and third-party data by replacing outdated servers and switches.
- ***Result 2:*** Enhance Museum staff members' cybersecurity knowledge and practices through general and targeted trainings, thereby decreasing the cybersecurity risks posed by insider threats.
- ***Result 3:*** Decrease the impact that potential cybersecurity events would have on the Museum and its visitors and enhance the responsiveness of the Museum website and servers to better serve visitors and staff.

Specific metrics and indicators of success will be set for these results at the start of the project following the establishment of baseline data during the cybersecurity assessment. See "Data Collection," below, for the methods that will be employed to measure these metrics. In addition, the SMARTS project will also directly contribute to the achievement of metrics from the Museum's strategic plan, as outlined above ("Advancing the Museum's Strategic Plan").

Changes in Knowledge, Skills and Behaviors:
The project will aim to institute good cybersecurity practices as an institution-wide priority across all departments. As a result of the SMARTS project's cybersecurity capacity building activities, Museum staff will have increased awareness of the importance of cybersecurity and will have the knowledge to identify and prevent attempted phishing scams, avoid malicious downloads, detect other types of threats, and immediately report any attempted or successful data breeches to the proper personnel. These changes in knowledge, skills, attitudes and behaviors will be measured through a rigorous evaluation and data collection process, as outlined below.

Data Collection:
As outlined above (see "Evaluation Activities"), the primary data to be collected by the SMARTS project are measurements of the Museum's cybersecurity performance as assessed by baseline, mid-term and end-line cybersecurity audits. Data from the audits will be key to measuring progress against all three project results. The project will also gather initial feedback from Museum staff participating in Cybersecurity Training 2.0 (Activity 2.2) via post-training questionnaires, which will measure changes in knowledge, skills, attitudes, and behaviors as well as the trainings' success in achieving learning metrics established during development of the training curriculum. This data will inform plans for targeted cybersecurity trainings or coaching sessions (Activity 2.3) to address cybersecurity capacity building needs that remain unmet. Finally, the Museum's IIT Team will also issue internal reports assessing the degree to which roll-out of Phases 2 and 3 of the Museum's IT Disaster Recovery Plan (Result 3 of this project) is successful.

Tangible Products:
The project will develop the following tangible products: (a) Cybersecurity audit reports at the baseline (pre-project), mid-term, and end-line stages; (b) A Museum-wide staff Cybersecurity training course, which will be shared with other Museums and arts and cultural institutions, as outlined above under "Results Dissemination;" (c) Procurement and installation of 3 new severs and 25 new switches; and (d) Off-site and cloud backups of mission-critical servers and data.

Sustainability:
The SMARTS project will support many of the up-front costs associated with enhancing the Museum's cybersecurity, including investments in on- and off-site infrastructure as well as staff capacities. Key equipment purchased under the project will have a lifespan of at least 7 years. Routine maintenance of these infrastructure investments will be incorporated in the Museum's annual IIT operating budget, and, in accordance with the Museum's IT Asset Management Policy introduced in 2020, a plan will be developed to ensure their replacement costs are budgeted in future years' operational budgets before maintenance costs begin to outstrip the cost of replacement. The Museum's annual operational budget is funded through diversified revenue streams that include earned revenue, a conservative annual endowment draw, and contributed revenue from individual, foundation, corporate, and government sources. Additionally, cybersecurity training assets produced under this project will be incorporated into standard staff training plans following the end of the project, ensuring the sustainability of project benefits.

"SAFEGUARDING MUSEUM ASSETS BY REVAMPING TECHNOLOGY & STAFF CAPACITIES"

SCHEDULE OF COMPLETION

Project Activity	2021				2022												2023												2024							
	09	10	11	12	01	02	03	04	05	06	07	08	09	10	11	12	01	02	03	04	05	06	07	08	09	10	11	12	01	02	03	04	05	06	07	08
ACTIVITIES CORRESPONDING TO RESULT 1																																				
1.1: Equipment Procurement	■	■																																		
1.2: Equipment Installation			■	■	■																															
1.3: Software Updates & Maintenance						■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
ACTIVITIES CORRESPONDING TO RESULT 2																																				
2.1: Recruit a Cybersecurity Expert	■	■																																		
2.2a: Staff Cybersecurity Training Development			■	■	■	■																														
2.2b: Staff Cybersecurity Training Roll-Out							■	■	■	■	■																									
2.3: Targeted Cybersecurity Training/Coaching												■	■	■	■	■	■	■	■																	
ACTIVITIES CORRESPONDING TO RESULT 3																																				
3.1: Off-site and Cloud Back-ups										■	■	■	■	■	■	■	■	■	■	■	■	■														
3.2: Bridging On-Site and Cloud Servers																				■	■	■	■	■	■	■	■	■	■	■	■					
EVALUATION ACTIVITIES																																				
4.1: Baseline Cybersecurity Audit (pre-project)																																				
4.2: Mid-Term Cybersecurity Audit															■	■	■																			
4.3: End-line Cybersecurity Audit (post-project)																																				