Incident Emergency Fund (IEF)
Deploy and Nurturing Gallery (DNG)

## Report on project titled

# THE CYBER SHIELD: ENSURING THE SAFETY AND INTEGRITY OF OUR DIGITAL ENVIRONMENT

**June – September 2023**

Submitted to;

Digital Defenders Partnership/HIVOS
The Hague,
The Netherlands
Email: team@digitaldefenders.org
Website: https://digitaldefenders.org

Report by;

Deploy & Nurturing Gallery (DNG)
P.O. Box 16450,
Arusha, Tanzania
Email: info@dng.or.tz
Mob: +255713004481
Website: https://www.dng.or.tz

September, 2023

# QUARTERLY UPDATE REPORT

**1. Please provide us with a brief update on progress made in your project to date. (Max. 500 words)**

The Deploy & Nurturing Gallery as growing organization had made a great progress after secure funds from HIVOS/DDP and become their partner in implement *the Cyber Shield: Ensuring the Safety and Integrity of Our Digital Environment project*. The project carried out within the period of three months started from June to September 2023. However, the actual project activities implemented in the period of July to August, 2023. Whereby, the planned project activities grouped into two major activities such as; Equipment's procurement and installation, and also capacity building workshop which ending drafting cyber safe guideline/policy of the organisation.

The progress made in the project within the said period are as follow, digital safety awareness training workshop, this is the cornerstone of the project was the capacity building training aimed at enhancing the digital safety awareness and skills of our staff, volunteers and local partners. Over the past three months (June to September, 2023). The five-day constructive workshop conducted and facilitated by the digital expertise. All 10 targeted participants attend the training session. The training covered a wide range of digital safety topics, including safe online behaviour, recognizing cyber threats, secure data handling, and best practices for maintaining a secure digital environment. We are pleased to report that all participants showed significant improvements in their understanding of digital safety concepts and their ability to identify potential threats. The training sessions received positive feedback from the participants, highlighting their increased confidence in navigating the digital landscape securely.

Organisation digital safety policy development, from the workshop under the collaboration with cybersecurity experts for the development of a comprehensive digital safety policy has been fruitful. The policy is in the final stages of drafting and will soon be ready by the end of October. It encompasses detailed guidelines, protocols, and best practices tailored to our organization's specific needs. This policy will serve as a crucial resource in ensuring a secure digital environment within our organization. The, policy will remain and the official document or manual to reminder and guiding staff, volunteers and partners on safe way of interacting with the digital environment and protect the work done by the organisation. This increased the staff confident, make them work freely and more secure, in the digital world.

Working infrastructure enhancement, also the significant achievement made by the project to the organisation was the successful procurement of essential computer equipment such as desktop, laptops, anti-virus, data storage devices, and the establishment of a secure internet connection. These improvements have significantly strengthened our organization's digital infrastructure. Staff members now have access to up-to-date computers and a secure internet connection, providing them with the necessary tools for secure online work.

**2. Are there any unforeseen changes in your situation that may merit a change to the project plan or budget? If so, please give details.**

As of the current project update, we have not encountered any unforeseen changes in our situation that would necessitate a change to the project plan or budget. The project has been progressing as initially outlined, with no significant deviations or unexpected challenges that would impact the allocated budget or project timeline. The team have maintained close monitoring of the project's implementation, ensuring that all activities are on track, and the budget is being utilized efficiently and effectively, by prioritising activities. The proactiveness approach to addressing challenges and potential issues has helped the organization stay aligned with the project's original objectives.

However, unforeseen circumstances of bank charges were noted and raise, although did not affect the project. The team remain vigilant and prepared to adapt to any unexpected changes should they occur. Our priority is to ensure the successful completion of the project while maintaining the quality and integrity of the activities outlined in the project plan.

**3. Please give details of the beneficiaries of the project to date on the table below. *These identities can be overlapping (e.g., a person may identify as more than one of the below categories). For this reason, the "total individuals" column may indicate less than the sum of the other columns*.**

In the table below shows the number of direct project beneficiaries, these are including all staff who direct participated in the workshop were seven females including program coordinator, gender officer, legal and empowerment officer, one volunteer, and two partners. Also, three males benefited from the project workshop include executive director, finance and administration manager, and one volunteer. However, the project will also benefit more than 20 people as indirect beneficiaries this referring to individuals who engage with the organisation.

| **Gender identities of beneficiaries** | **Female-identified** | **Male-identified** | **Trans*-/Intersex/Non-binary** | **Other/Rather Not say** | **Total Individuals** |
|---|---|---|---|---|---|
| How many individuals benefitted directly from this project (e.g. participants in workshops, organization staff or volunteers, etc). | 7 | 3 | - | - | 10 |

| **Types of human rights work / activism of beneficiaries** | **Number of beneficiaries** |
|---|---|
| People who make information available for the public (e.g., journalists, bloggers, whistle-blowers, etc) | 1 |
| LGBTIQ+ rights defenders | - |
| Women's rights defenders | 4 |
| Environmental / Land / Indigenous Rights defenders | 1 |
| Other Civil & Political Rights defenders | 3 |
| Other Economic, Social, Cultural Rights defenders | 1 |
| Other | - |
| **Total Individuals** | **10** |

## Final Narrative Reporting Format

**Please indicate the level of confidentiality you prefer for this report:**

- **Public**: I am happy for details of this project to be shared publicly in reports to donors, public blogs or case studies published on DDP's webpage (in any case names of individuals will never be published, only those of organisations involved in the coordination of the activity)
- **Private**: I am happy for details of this project to be shared publicly in reports to donors' public blogs or case studies published on DDP's webpage *without mentioning the names of the organization(s) or individuals involved*.
- **Confidential**: I request that information about this project not be shared in any form except confidentially (without names) towards DDP donors.

## A. Description of activities and impact

***1. What activities were carried out as part of this project? Check all relevant boxes.***

☐ *A needs assessment in order to identify my/our needs in more detail.*
☒ *Purchase of software licenses.*
☒ *Purchase or repair of IT hardware (e.g. computers, hard drives, etc).*
☒ *Secure external hosting or other infrastructure.*
☐ *Support to maintain, archive or safeguard databases or other sensitive information.*
☐ *Response to an internet shutdown*
☐ *Response to censorship or a website takedown*
☐ *Response to online harassment*
☒ *Improvements to internal hosting or infrastructure.*
☐ *Purchase of other hardware related to security.*
☒ *Training workshops on digital security.*
☐ *Other digital security support or accompaniment.*
☐ *Training or workshops on physical security.*
☐ *Other support or accommodation on physical security.*
☐ *Training or workshops on psychological or psychosocial well-being*
☐ *Other support or accommodation on psychological or psychosocial well-being*
☐ *Legal or paralegal support*
☐ *I don't know / other (please detail in the next question)*

**2. Please provide a narrative description of the activities carried out. (Max. 500 words)**
During the project's three-month duration, a series of carefully planned activities were executed to achieve the objectives of Ensuring the Safety and Integrity of Deploy and Nurturing Gallery (DNG). The following narrative provides an overview of the activities undertaken:

**Activity 1; Procurement of working equipment's and installation of the Internet facilities**
To ensure staff had the necessary tools for secure online work, the project successfully procured working tools like computers, anti-virus, data storage device and data backup. Also, the established a secure, high-speed internet connection within the organization office. This infrastructure upgrade was essential in providing staff with a secure digital environment. The procurement process involved meticulous vendor selection, negotiation, and quality assurance checks to ensure that the purchased equipment met our organization's requirements. The new computers and internet facilities have significantly improved our staff's efficiency and security in their digital workspaces.

**Activity 2; The capacity building training workshop**
The cornerstone of our project was the capacity building training session, designed to enhance the digital safety awareness and skills of our staff members, volunteers and local partners. Over the course of project duration, five-day workshop conducted and total of 10 participants attended the training sessions. The session was structured to accommodate the schedules of the participants, ensuring maximum and active participation.

- Some of the training session subjects including, safe online behaviour, here the participants were educated on the importance of responsible online conduct, emphasizing the need for strong and unique passwords, safe email practices, and the avoidance of suspicious websites and links.
- Recognizing cyber threats, training sessions included practical exercises to help participants identify common cyber threats such as phishing emails, malware, and social engineering tactics. real-world examples and case studies were used to illustrate these threats especial the attack the DNG experienced.
- Secure data handling, workshop participants were also trained in best practices for handling and protecting sensitive data. This included secure file storage, encryption, use strong password, using password safe, and secure data disposal methods.

The training was highly interactive, with participants actively engaging in discussions, group activities, and scenario-based exercises. Feedback from participants indicated a significant improvement in their digital safety awareness and confidence in navigating the digital landscape securely. The training also provides some suggestions to the development of organisation digital safety policy. All participants and cybersecurity experts work together and assist in developing a

comprehensive digital safety policy tailored to Deploy and Nurturing Gallery's specific needs. The policy development process involved, the conducting a thorough assessment of our organization's digital environment, identifying vulnerabilities and potential risks. Collaborating with key stakeholders to define the scope and objectives of the policy. Researching and incorporating industry best practices and legal compliance requirements. Drafting clear and concise guidelines, protocols, and procedures to address digital safety concerns.

The policy is currently in the final stages of drafting and is expected to be ready for implementation in the near future. It will serve as a crucial resource to ensure a secure digital environment within our organization.

**3. What was the impact of this project on your security situation (or that of the beneficiaries, if different to you)? (Max. 500 words)**
The project, generously funded by the Digital Defender Partnership (DDP) and Hivos, has had a significant and positive impact on our organization's cybersecurity posture. This impact extends not only to the organisation but to its beneficiaries as well.

**Enhanced digital safety awareness**
The project's capacity building training sessions have played a pivotal role in raising the digital safety awareness of staff. As a result of the training, staff members have developed a deeper understanding of digital safety concepts, recognizing the importance of safe online behaviour, secure data handling, and the identification of cyber threats. Increased vigilance and awareness among staff have led to a substantial reduction in incidents related to phishing attempts and other cyber threats. This has directly contributed to a more secure digital environment.

**Fortified digital infrastructure**
The procurement of new computers and the establishment of a secure internet connection have significantly enhanced organization's digital infrastructure and increased confidence of staff to work in a digital environment. The impact includes, improved efficiency and productivity among staff members due to access to up-to-date and reliable computer equipment. A more secure digital work environment with robust protection against malware and cyberattacks, thereby safeguarding our sensitive data and confidential information.

**Comprehensive digital safety policy**
The development of a comprehensive digital safety policy tailored to the organization's needs has been a transformative milestone. The policy's impact is twofold will provide a clear guidelines and protocols outlined in the policy provide staff members with a roadmap to follow in ensuring digital safety. This ensures consistent and standardized practices across the organization. The policy serves as a proactive measure to mitigate potential cyber risks and vulnerabilities, safeguarding our organization's digital assets. It also ensures regulatory compliance and data protection in alignment with best practices.

The cyber shield ensuring the safety and integrity of our digital environment project has made a substantial and lasting impact on DNG's cybersecurity. It has empowered staff, volunteers and partners with the knowledge and tools necessary to navigate the digital landscape securely, improved digital infrastructure, and established a comprehensive digital safety policy framework.

**4. How do the results mentioned above compare with the results you had planned to achieve with this project (better than expected, worse than expected)? (Max. 250 words)**
While the project's progress and outcomes align closely with our initial expectations, the extent to which staff members embraced and implemented digital safety practices was particularly encouraging. The project's impact on staff vigilance and behaviour in the digital space has exceeded the expectations, reinforcing the effectiveness of the training session. Overall, the project has not only achieved its objectives but has also set a strong foundation for ongoing cybersecurity measures and digital safety awareness within our organization.

Staff's improved understanding of digital safety concepts and their ability to identify cyber threats. The training sessions were highly effective in raising awareness, and staff members exhibited a strong commitment to implementing safe online practices. While the drafting of the digital safety

policy took some time, the resulting document is comprehensive, tailored to our organization's specific needs, and aligns with industry best practices. The thoroughness of the policy's guidelines and protocols was better than expected. The procurement of computers and the establishment of a secure internet connection were executed seamlessly and within budget. The impact on staff productivity and the overall security of our digital environment exceeded our initial projections.

**5. How were the particular needs of beneficiaries arising from their gender identity, sexual orientation, ethnicity, race, ability, caste, or other characteristics addressed in this project? (Max. 500 words)**

The project was designed with a strong commitment to inclusivity and diversity, recognizing that the needs of beneficiaries may vary based on gender identity, sexual orientation, ethnicity, race, ability, caste, or other characteristics. Team implemented several strategies to ensure that the project addressed these specific needs effectively during the project implementation duration.

Inclusive training approach. The employed an inclusive and culturally sensitive training approach that respected the diverse backgrounds of our staff. The training content and materials were carefully curated to avoid any biases, stereotypes, or offensive content related to gender identity, sexual orientation, ethnicity, race, ability, or caste. The project implementation also, fostered an open and inclusive training environment where all participants felt comfortable expressing their views and concerns.

Tailored communication. Recognition of the importance of clear and tailored communication. Project updates, training materials, and policy documents were provided in multiple languages Swahili and English to accommodate participant especial volunteers and local partners with varying linguistic backgrounds.

Diversity in training delivery. The selection and engagement of the facilitators who were sensitive to diversity and inclusion issues. These trainers ensured that the training sessions were conducted in a manner that respected and acknowledged the unique perspectives and experiences of each participant. They actively encouraged open dialogue and created a safe space for discussing sensitive topics related to gender, identity, and inclusivity in the digital realm.

Equal access to resources. In the procurement of computers and internet facilities, we ensured equal access for all staff members, regardless of their abilities or special requirements.

Inclusivity in policy development. The development of the digital safety policy was an inclusive process, opinion and inputs from a diverse group of participants, including those who may have unique concerns related to their differences. Their perspectives were actively considered in shaping the policy to ensure that it was sensitive to their needs.

Continuous feedback mechanism. We established a feedback mechanism that allowed staff members to share their thoughts and concerns throughout the project. This enabled us to make real-time adjustments to our approach and address any issues or barriers faced by specific groups of beneficiaries. By actively integrating these strategies into the project, we aimed to create an environment where all beneficiaries, regardless of their characteristics, felt respected, included, and empowered to participate fully in the project's activities. The organisation commitment is to diversity and inclusivity was central to our approach, reflecting our organization's dedication to equity and social justice.

**6. Do you have any important lessons learned from implementing the project? (Max. 500 words)**

Through the implementation of the cyber safety project, we have leaned several important lessons that can inform our future endeavours and contribute to the broader field of cybersecurity and digital safety;-

The power of inclusive training, we learned that an inclusive training approach not only respects diversity but also fosters a more effective learning environment. By acknowledging and addressing the unique needs of participants, we are going to create a training program that resonated with a wider audience. Inclusivity not only enhances engagement but also improves the retention of digital safety knowledge.

The value of real-world scenarios, incorporating real-world scenarios and case studies into our training sessions proved highly effective. These scenarios allowed participants to apply their knowledge in practical contexts, enhancing their ability to recognize and respond to cyber threats. We will continue to utilize this approach in future training programs, as we planned to escalate the knowledge on cybersecurity.

Adaptability in cybersecurity, the ever-evolving nature of cyber threats demands adaptability. We learned that cybersecurity measures should be dynamic and flexible to address emerging threats effectively. Staying updated on the latest cybersecurity trends and continuously reviewing and updating our policies and practices is essential.

Inclusivity in policy development, inclusivity in policy development is crucial. Engaging a diverse group of stakeholders enriched the quality and relevance of our digital safety policy. Ensuring that policies consider the needs and concerns of all individuals and communities they impact enhances their effectiveness and legitimacy.

Collaboration with experts, collaboration with cybersecurity experts was invaluable in policy development. Their expertise and insights provided a deeper understanding of potential threats and vulnerabilities specific to our organization. Engaging external experts in cybersecurity is a practice we will continue to prioritize.

Importance of feedback mechanisms, establishing a robust feedback mechanism allowed us to address issues promptly. Regular feedback from staff members was instrumental in identifying areas for improvement and ensuring that the project remained responsive to their needs and concerns.

Long-term sustainability, sustainability in cybersecurity efforts is critical. We recognize that maintaining a secure digital environment is an ongoing process. To sustain the positive impact of this project, we plan to implement regular refresher training sessions and conduct periodic reviews of our digital safety policy.

Empowerment through education, one of the most significant lessons learned is the transformative power of education in cybersecurity. Empowering individuals with knowledge and skills to protect themselves and their organizations from cyber threats is not only a defensive measure but also an empowering one. It enhances digital literacy and enables individuals to participate confidently in the digital world.

In conclusion, this project has provided valuable insights into the multifaceted nature of cybersecurity and the importance of inclusivity, adaptability, and collaboration in digital safety efforts. These lessons will guide our future initiatives and contribute to our organization's ongoing commitment to maintaining a secure digital environment and promoting digital safety awareness.

## B. Beneficiaries & Overall Evaluation

**These identities can be overlapping (e.g. a person may identify as more than one of the below categories). For this reason, the "total individuals" column may indicate less than the sum of the other columns.**

| Gender identities of beneficiaries | Female-identified | Male-identified | Trans*-/Intersex/Non-binary | Other/Rather Not say | Total Individuals |
|---|---|---|---|---|---|
| How many individuals benefitted directly from this project (e.g. participants in workshops, organization staff | 7 | 3 | - | - | 10 |

| | | | | | |
|---|---|---|---|---|---|
| or volunteers, etc). | | | | | |

1. **Please give your estimated breakdown of the kinds of work carried out by beneficiaries of the project. *These identities can be overlapping (e.g. a person may identify as more than one of the below categories). For this reason, the "total individuals" row may indicate less than the sum of the other rows.***

| Types of human rights work / activism of beneficiaries | Number of beneficiaries |
|---|---|
| People who make information available for the public (e.g. journalists, bloggers, whistleblowers, etc) | 1 |
| LGBTIQ+ rights defenders | - |
| Women's rights defenders | 4 |
| Environmental / Land / Indigenous Rights defenders | 1 |
| Other Civil & Political Rights defenders | 3 |
| Other Economic, Social, Cultural Rights defenders | 1 |
| Other | - |
| Total Individuals | **10** |

*The following questions are for the beneficiaries of the project. If the project was carried out internally, please answer them yourselves. If your project was aimed at supporting a third person/group/organisation (e.g. through training, creation of resources, etc) please gather this data from the beneficiaries themselves as part of your own evaluation.*

Please check the box which most closely corresponds to your evaluation of the project.
***3.1. Have your security capacities improved as a result of this project?***
☒ Yes, very much ☐ Yes, sufficiently ☐ No change ☐ Not sufficiently ☐ Not at all

*Please elaborate briefly on your answer: if your capacities have improved, how and why? If your expectations have not been met, why?*

***3.2 Has this project helped sustain your work (or that of beneficiaries)?***
☒ Yes, very much ☐ Yes, sufficiently ☐ No change ☐ Not sufficiently ☐ Not at all

***Please elaborate briefly on your answer:***
Yes, this helped very much sustain the staff and the entire organisation as general. Because all the intended working equipment's were procured, install and works; the knowledge of staff on cybersecurity increased and they practising it.

***3.3. Did this Incident Emergency Funding and the activities carried out respond effectively to the threats you face (or those of the beneficiaries, if different to you)?***
☒ Yes, very much ☐ Yes, sufficiently ☐ No change ☐ Not sufficiently ☐ Not at all

***Please elaborate briefly on your answer:***
Using own internet services, computers equipped with anti-virus all of those respond effectively to the threats the organisation experienced. Also, migrate hosting from the add-on cPanel shared account to the separate account, which is more secure single cPanel this increased the security of the organisation website and its data. At the same time respond to cyber security threats, faced before.

## C. Other Indicators (Optional)

**Please share here any other information that you think demonstrates the impact of the project (e.g. other indicators and data you have collected).**