CSIRT Overview

[Name of the Writer]

[Name of the Institution]

CSIRT Overview

# Vision and Mission of the CSIRT

 The CSIRT is the governmental initiative that tends to make sure that the systematic and organized response is provided to the security threats and the incidents that are faced by the organizations at the given point of time. The idea is to make sure that the private sector, the communities’ organizations as well as the non-governmental entities are going to be in the position to make sure that they are able to take care of themselves. Keeping these objectives in mind, following are the vision and mission of CSIRT. The mission statement of the CSIRT is as followed. Their mission is to

Our mission is to:

* provide a systematic rBEEesponse facility to ICT-incidents
* coordinate communication among national and international incident response teams during security emergencies and to help prevent future incidents
* support ICT users in Luxembourg to recover quickly and efficiently from security incidents
* minimize ICT incident-based losses, theft of information and disruption of services at a national level
* gather information related to incident handling and security threats to better prepare future incidents management and provide optimized protection for systems and data
* provide a security related alert and warning system for ICT users in Luxembourg
* foster knowledge and awareness exchange in ICT security

#### “Eearly Detection, Prevention, and Response to computer security incidents” and raise cyber security awareness in public and private organizations and the general public.”

• Serve as a National Point of Contact (POC) for computer security incidents coordination and response.
• Provide accurate and timely information on current and emerging cyber security threats and vulnerabilities.
• Build Rwanda Cyber Security capacities to handle cyber security incidents and threats
• Promote information security awareness with the aim of building cyber security culture for internet users in Rwanda.
• Promote Research and Development in the cyber security field.
• Promote Regional and International cooperation in the field of cyber security.

# Key Stakeholders that CSIRT is supposed to Serve

 There are many key stakeholders that the CSIRT is supposed to be serving. One of the reasons that the scope of the service is so broad is due to the fact that they are one of the few organizations that have the capacity and the infrastructure to make sure that the protection can be provided from the impending information security threats. Following are some of the stakeholders that they are going to be serving.

* Government Organizations: These are the primary beneficiary of the range of the services that are provided by the CSIRT. It has the special protocols for the people who belong this sector.
* Private Organizations: CSIRT acts as a business consultancy that acts to make sure that the private organizations are also aided when it comes to how they are going to be making sure that the right service is going to be provided to different organizational stakeholders at the given point of time.
* Communities: The communities and the NGO’s are another sector that CSIRT intends to serve. The idea is to make sure that the integrated solution is provided to these stakeholders.

# It provides a reliable and trusted point of contact for any users, companies and organizations based in Luxembourg, for the handling of attacks and incidents. Its team of experts acts like a fire brigade, with the ability to react promptly and efficiently whenever threats are suspected, detected or incidents occur.

# Scope and the Level of Service of the CSIRT

 As discussed in the previous section, they are the organization that is involved in the development of the security protocols and service for the organization. The scope of the business is to make sure that the complete IT security solutions is being provided to the organizations at the given point of time. Now, when one talks about the scope of services of the organization, following are some of the services that are provided by the organization.

* Management of the risk and the analysis of the IT security risk that is provided by the organization at the given point of time.
* Making sure that there is sense of continuity in terms of how the disaster recovery planning is needed to be done by the organization.
* Helping the organizations to make sure that they are able to carry out the compliance audits as well as make sure they are able to make the security assessment related to the organizational safety.
* Carrying out the SOC analysis and allowing for the development of the security architecture analysis of the organization at the particular point of time.

# Staffing Requirement at the End of the Organization

 One key thing that has to be noted about CSIRT is that the range of the services that are provided by the organization, they are quite limited in terms of how they tend to add out as far as the way overall analysis is needed to be provided. The idea is there among the broader stakeholders when it comes to making sure that the personnel requirement has to be quite optimum and there is no need for excessive hiring at the end of the organization. Now, keeping in mind the range of services that are provided by the organization. People who are well equipped with the IT security and network security protocols are the ones that would play an important role in terms of the operations of the organization. At the same time, having an insight about the designing of the architecture of the entity in terms of the networking is another one of the services that are provided at the end of the organization. The people who are on board are also needed to be well accustomed with the effective control analysis. For example, the cyber risk created by the acquisition of robots in the organization’s warehouse has been identified and assessed by the experts (CISO and CRO with the concurrence of the CIO) as high, more than they believe the organization should take. Note, I use “take risk” rather than “accept risk” as it is more true to real life and the decisions we have to make.

# Existing Security Technical Staff and Resources

 One of the key things that has to be kept in mind with regards to this business is that the resources are needed to be quite optimum. At the moment, the CSIRT is operating at a very limited scope and thus it is quite important for them to make sure that have a sense of insight with regards to what are some of the HR requirements that they have need for at the moment. The resource constraints though are one of the areas that they need to work upon. The problem for them is that how the determination of the resources is going to be done. Most of the times it becomes quite confusing when it comes to making sure that the right balance is adopted. What can be done by them is to make sure that they need to setup an IT asset management protocol that goes a long way towards how the management of the resources is going to be done at the given point of time. The idea is to make sure that the how the assessment of the risk is going to be done and thus need by need analysis is required in this instance. They worked with business managers to reach this decision and based the risk assessment on how a breach would affect enterprise objectives.

# Example of the External Resource Needed

 During the course of the organizational goal implementation, there is a need to make sure that how the determination of the external resources is going to be done at the level of the organization. The among all the broader stakeholders is to make sure that how the right balance is going to be done in terms of the acquisition and the need assessment is going to be needed. For instance, there might be a case where the people at the CSIRT are required to intervene and create and IT infrastructure. To make sure that this infrastructure is created in the right manner, the whole network output criterion was needed. Now, it would have been quite needless for them to make sure that they use this asset when they don’t have any need for it at the first place. So, what was done by the CSIRT was to make sure that none of the assets were purchased, but instead whenever there is a need for the heavy asset, they tend to lease it out.

# Top Five Policies and Procedures

 There are range of the policy and the procedures that are carried out by CSIRT at the given point of time that would make sure that how the readiness level of the business is being determined, and thus the proactive services that they are providing is one of the most important procedure that they are providing to the stakeholders. At the same time, another range of procedure that plays an important role in the client value preposition is the way secure quality management ideals are being provided and how the services are being made possible at the given point of time. This is an important aspect of the services of the CSIRT. Then there is service augmenting that tends to make sure that the existing protocols that are setup at the end of the organization are such that are going to be good enough to make sure that the independent handling is going to be provided to the stakeholders without resorting to the issue of the lack of handling that is faced by the businesses at the given point of time. The training modules and the IT audits are also important procedures.

# Reporting Structure and Organizational Model

 Now, when one talks about the organizational model that is being used during the course of the operations of the CSIRT, the key thing that tends to stand out is that how different it is as compared to some of the traditional organizations. The reason for this difference exists due to the fact that the range of the services that are provided by them are such are quite exclusive in nature and due to that, it is imperative that some sort of insight is developed in terms of how it is going to be made sure that the right structure and defiance level is going to be seen. Most of the times, when one talks about the organizational structure that is being used by the organizations of such magnitude and scale, it is imperative to make sure that the functional structure is used. The advantage and the core reasons that the CSIRT has been using the functional structure is due to the fact that it is one of the few organizations that is quite different in terms of the functionality and how it operates. The other aspect that is needed to be kept in mind is that their range of services are quite heterogeneous and one tone, so a need is not there for complex reporting and organizational structure.

# Amount of Additional Funding Implement and Maintain CSIRT

 One of the key things that is needed to be kept in mind with regards to the way funding requirement is going to be carried out is that what are the current operational modules that are faced by the organization at the given point of time. The effort is needed to be made to make sure that the sense of perspective is needed to be there in terms of how funding is needed to be done. At the moment, the structure of the organization is such that they do not have need for the long term financing, and as majority of the assets can be leased, and not much need for the heavy machinery, one of the thing that can be done by them is to make sure that they take care of their funding requirement with the help of the internal funding and the debt consideration is not needed to be there.

# Communication Plan for the Business

 One of the thing that is needed to be kept in mind is that still to this date, the organizations at the government level are not really aware of what are some of the security risks that are faced by them at the given point of time and how the sense of balance can be achieved in this regard. So, the first thing that is needed to be done at the level of the organization must be to make sure that all the required stakeholders are communicated about the business need in an appropriate manner. What it means is that the effort must be made to make sure that the sense of perspective is needed to be there in terms of how the assessment of the organizations need is going to be done. Not only that, the other key thing that is quite important in this regard is to make sure that all the organizational stakeholders are in the position to determine the effectiveness and the benefits that the financial states are going to be gaining if they are working with the CSIRT. They must be made to realize the value preposition of adding the CSIRT to their panel. Top management and the board should have serious conversations that focus not only on acceptable losses, but also on what investors and regulators might consider a reasonable level of cyber defense, detection and response. Any definition of ‘risk appetite’ should probably be based on the likelihood of a serious breach, rather than on the amount of loss.

# Timeline for the Implementation of the CSIRT

 It has to be noted that when one talks about the timeline, it is quite hard to make sure that the exact timelines are being communicated. One of the reasons that the whole process is quite hard to be achieved is due to the fact that how the whole information serving protocol is needed to be looked at the given point of time and what are some of the long term implications of such a business decision at the given point of time. So, the management of the resources is quite important when such a consideration is needed to be made. Now, for a small business, it is quite possible that this timeline can be determined and as per estimates and the past instances when the whole protocol was being implemented, it takes about two quarters or about six months to make sure that the correct assessment is being made in this regard. The idea is to make sure that the sense of balance has to be there in terms of allocation of resources.

# Return on Investment for Implementation of CSIRT Standards

 It has to be noted that whenever such an investment is being carried out, the ideal thing that can be done at the level of the organization is to make sure that the whole thing is needed to be looked at in terms of its totality. The idea is to realize that how the whole thing is going to add value in terms of how the investment at the cybercrime level is going to be carried out. For instance, there are risks that are associated with the acquisition of the bots and other particulars and it is very important to make sure that these risks are accounted for when the decision is being made. Looking at the numbers, the current risk that the entity would be facing in terms of the state government would be around $ 10 million or it can be said about the 5 per cent of the total risk profile of the organization at the given point of time specifically when the investment is in place. What it means is that the ROI in this instance would be around 2 per cent of the whole equation or it can be 3 per cent that equals about $ 300,000 at the given point of time. This seems to sound like a great investment and keeping in mind the amount of losses and the risk profile that is faced by the organization, it is safe to assume that the such a decision would work out for the long term future of the organization to say the least.

# Examples of Cyber Security Incidents

 There have been many examples in the past that how the cyber security incidents have curtailed the long term health of the organization. The biggest example that comes to mind in this regard is that of the NHS, when the confidential data of the patients was stolen and even though at that point of time, it was not considered to be that huge of an investment, when the social security numbers of the students were obtained by the people at the given point of time, they were able to reflect upon the same scenario at the particular point of time.

# Total Cost of the Incident

 The final thing that is needed to be kept in mind is that how the total cost of such an incident is going to be worked out. Now, there are some important considerations that are needed to be looked at when this determination of the cost is being made. The first thing is that what is going to be the cost of the data that is being compromised at that point of time. The other thing that is quite important is that loss of the equipment and other aspects that are important when it comes to the way decisions about the long-term sustainability of the IT equipment is needed to be made. There is potential cost that is needed to be looked at in terms of what are some of the business opportunities that are lost by the organization at the given point of time and how it is is going to eventually add up at that point of time. There are some indirect costs as well such as the potential loss of the goodwill for the business and how the resource allocation constraints are going to be faced by the business at the corresponding point of time.

**References**

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2016). *Defining incident management processes for csirts: A work in progress* (No. CMU/SEI-2004-TR-015). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Bada, M., Creese, S., Goldsmith, M., Mitchell, C., & Phillips, E. (2017). Computer security incident response teams (CSIRTs) an overview. *Global Cyber Security Capacity Centre*, 1-23.

Dsouza, Z. (2017). Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security. *Fed. Comm. LJ*, *69*, 201.

Mejía, J., Muñoz, M., Ramírez, H., & Peña, A. (2016). Proposal of content and security controls for a CSIRT website. In *New Advances in Information Systems and Technologies*(pp. 421-430). Springer, Cham.

Renato, C., & María, N. (2015, July). Technologies' Application, Rules, and Challenges of Information Security on Information and Communication Technologies. In *2015 Asia-Pacific Conference on Computer Aided System Engineering*(pp. 380-386). IEEE.

Wara, Y. M., & Singh, D. (2015). A guide to establishing computer security incident response team (CSIRT) for national research and education network (NREN). *African Journal of Computing & ICT*, *8*(2), 1-8.