ACCEPTANCE OF INFORMATION SECURITY RESPONSIBILITY

I, the undersigned, _____, working with Nuvama, having read the Information Security Policy & the Acceptable Use policy, accept the responsibility of:

Physical Access:

- using all the physical accesses of the facility provisioned to me judiciously and only to the extent of my role. I will ensure that this privilege is not misused by knowingly or unknowingly allowing unauthorized individuals to enter areas of the facility unless authorized by my reporting authority.

Information:

- ensuring that I will not disclose or share any *information*, known by me through direct and / or indirect sources, through *unauthorized data channels*
- understanding that *information* gathered during my tenure at Nuvama or document created by me as part of my job responsibilities is the intellectual property of Nuvama and I shall have no claim over the *information*
- ensuring that *information* will be processed, stored and shared through channels authorized by Nuvama
- I understand that any *information* generated using Information systems or by me could be of sensitive nature and can have serious repercussions incase this is shared with *unauthorized individuals*.
- In case I am not aware who is authorized for sharing *information*, I will contact my Nuvama Reporting Authority before sharing, even if it means sharing it within my organization.

Information Systems:

- ensuring judicious usage of all Information Systems and services, authorized for use, as per Nuvama Information Security Policies.
- Systems not provisioned to me are considered as unauthorized for me and I will not be using these systems. In the event I accidently gain access to such systems, I will not misuse this access and immediately report this anomaly to my Nuvama Reporting Authority for further action.

Security Incidents:

- reporting any anomalous activity, including but not limited to, attempts to gain unauthorized access to systems, share *information* to unauthorized individuals, sharing of user ID and password, theft of *IT assets*, virus infection or anomalous behavior observed on Nuvama *Information Systems*, observed in the facility which can cause damage to the assets at Nuvama or cause harm to its employees
- co-operating with the team involved in case of a security event demanding investigation

I provide my consent to monitor all activities and all communications originating from and terminating to an Nuvama owned asset or an asset used to create, process and store Nuvama information.

If I have any further queries / clarifications concerning the above as applicable to me for my job, I know I can consult the Information Security Group at ISG@nuvama.com or Reporting Authority at Nuvama.

Information: Sensitive business data of Nuvama group companies and vendors or personal data of clients and employees

- Unauthorized data channels: non-Nuvama email, personal email, USB, CD-DVD, cloud storage
- Authorized data channels: Nuvama email, Nuvama file sharing application and any other business approved software
- Data Leak: unauthorized transfer of Nuvama data over unauthorized data channels
- Unauthorized individuals: Individuals not authorized to use Nuvama Information systems or handle Nuvama Information
- Information systems: Nuvama provided desktop, laptop, servers, databases, any other equipment used to store and process information
- IT Assets: Nuvama provided phones (landline & mobile), printers, and computer peripherals