KERALA POLICE
CYBERDOME
Public-Private Partnership for Cyber Security

Partner us
in making
a secure cyber world

Document ID: CYBDM-HR-001

Cyberdome Volunteer Framework

Version 1.1

Revision History

Version Number	Release Date	Description	Author	Reviewer	Approver
1.0	07-Nov-2017	Baselined	AnilKumar KG	Prakash SP	Manoj Abraham IPS
1.1	01-05-2019	Updated Self-Assessment document clause & Review	Rajeev R P	Prakash S P	Manoj Abraham IPS

Contents

1.Volunteer Structure

Category	Title	Responsibility	Cyberdome Reporting	ID Cards (One ID card will only be provided to each Volunteer)	ID Card Validity
Information Security Management Committee (ISMC)	Information Security Advisor	Advisory Committee responsible to review &advice information security compliance & governance of Cyberdome. This team is responsible to review organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.	Nodal Officer	Yes	2 Years
Cyberdome Commanders	Cyberdome Project Governing Council Member	Senior professionals responsible for reviewing / overseeing Cyberdome projects / Initiatives	Operations Officer	Yes	2 Years

	Commander	Senior professionals accountable for driving a function/project/initiative	Operations Officer	Yes	2 Years
	Deputy Commander	Manages/Responsible for execution of specific function/projects	Operations Officer	Yes	1 Year
	Assistant Commander	Manage team of volunteers assigned for specific function/projects	Operations Officer	Yes	1 Year
	Junior Commander	Volunteers working on assigned projects/tasks, Manage team of volunteers assigned for specific function/projects	Operations Officer	Yes	1 Year
Cyberdome Volunteers	Elite Member	Volunteers working on assigned projects/tasks.	Cyberdome Police Officers	No	NA
	Volunteer	Volunteers working on assigned projects/tasks	Cyberdome Police Officers	No	NA
Project Student / Trainee / Associate	Intern	Students/Research Scholars/ Trainee/Associate working on Research /Development projects	Cyberdome Police Officers	Yes* (* Temporary ID Card)	Internship Period

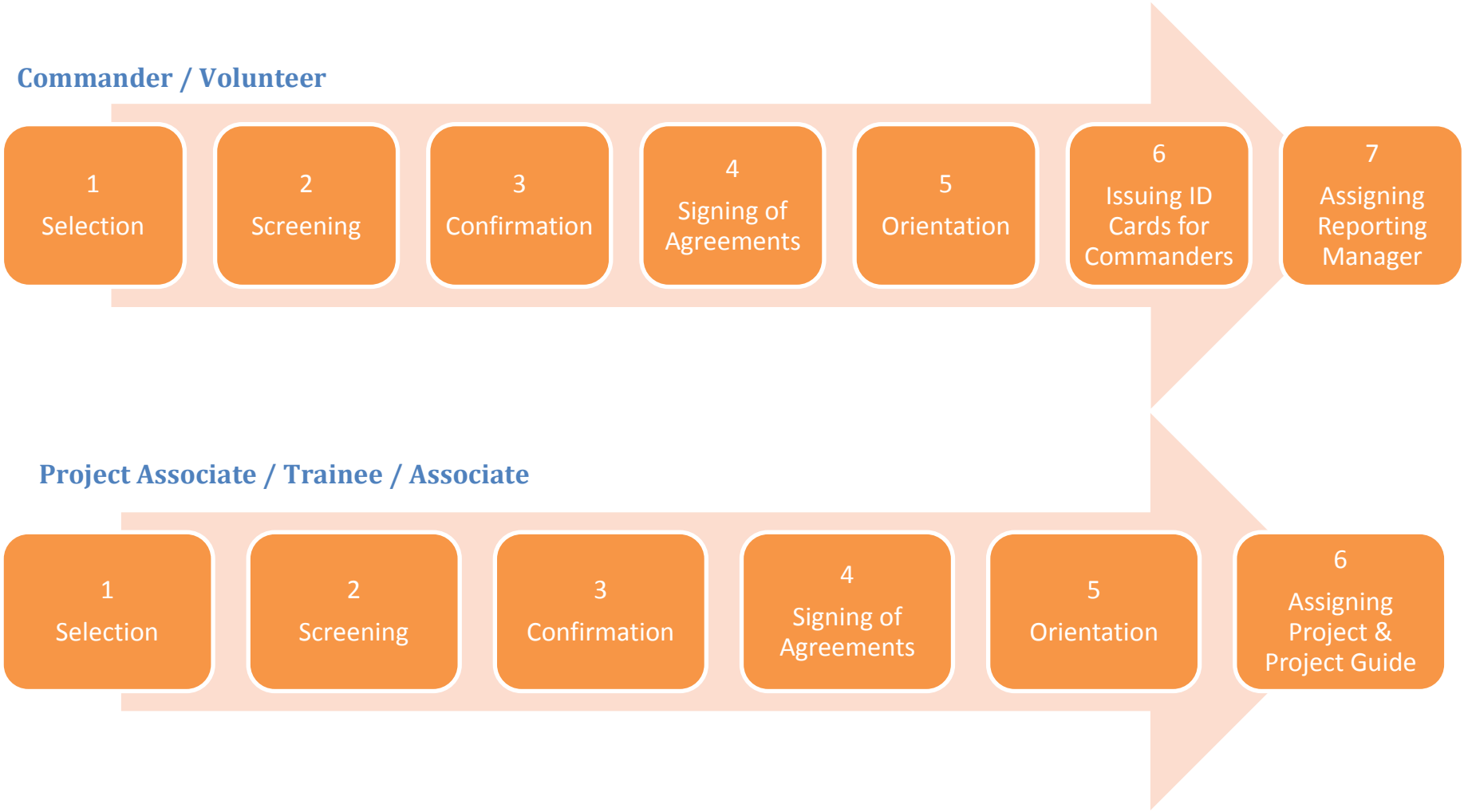
2.On Boarding Process

Title	Entry Criteria		Onboarding Requirements		Access to Cyberdome
	Direct	Promotion	Background Screening	Agreements	
Information Security Advisor	15+ Years of experience in Cyber Sec / Compliance Leadership / ISMS Auditor	NA	Govt ID verification Criminal History Check Social Media ProfilingApproval/Attestation	NDA Volunteer Framework Volunteer Agreement	Access limited to Internal/Confidential informationof Cyberdome other than investigation data, with approval from Nodal Officer. Physical: Vendor/Visitor Access only with escort
Commander/Cyberdome Project Governing Council Members	12+ Years of experience in Cyber Sec / Compliance Leadership / Academics	25+ quantifiable* work contributions to Cyberdome as a Deputy Commander with excellent service	Govt ID verification Criminal History Check Social Media ProfilingApproval/Attestation	NDA Volunteer Framework Volunteer Agreement	Access limited to Internal/Confidential informationon specific projects involved, with approval from reporting Cyberdome Officer. Physical: Vendor/Visitor Access only with escort
Deputy Commander	10+ Years of experience in Cyber Sec / Compliance	15+ quantifiable* work contributions to Cyberdome as an Asst Commander with excellent service	Govt ID verification Criminal History Check Social Media ProfilingApproval/Attestation	NDA Volunteer Framework Volunteer Agreement	
Assistant Commander	7+ Years of experience in Cyber Sec / Compliance	10+ quantifiable* work contributions to Cyberdome as a Junior Commander with excellent service	Govt ID verification Criminal History Check Social Media ProfilingApproval/Attestation	NDA Volunteer Framework Volunteer Agreement	
Junior Commander	4+ Years of experience in Cyber Sec / Compliance	7+ quantifiable* work contributions to Cyberdome as an elite member with excellent service	Govt ID verification Criminal History Check Social Media Profiling Approval/Attestation	NDA Volunteer Framework Volunteer Agreement	

Elite Member	3+ Years of experience in Cyber Sec / Compliance	5+ quantifiable* work contributions to Cyberdome as a Volunteer with excellent service	Govt ID verification Social Media Profiling Approval/Attestation	NDA Volunteer Framework Volunteer Agreement	Access limited to Internal information on specific projects involved with approval from reporting Cyberdome Officer. Physical: Vendor/Visitor Access only with escort
Volunteer	2+ Years of experience in Cyber Sec / Compliance Leadership.		Govt ID verification Social Media Profiling Approval/Attestation	NDA Volunteer Framework Volunteer Agreement	
Project Student/Trainee/ Associate	Technology students selected through screening/selection process	NA	Govt. ID proof. Recommendation letter & course certificate from college, previous mark lists etc. Social Media Profiling Approval/Attestation	NDA Volunteer Framework Volunteer Agreement Declaration	No access to Cyberdome Internal/Confidential information. Physical: Vendor/Visitor Access only with escort

*Quantifiable work – The quantifiable work may be any modules/project/activities/tasks/knowledge sharing sessions/training to Cyberdome Officers/idea/solution/ or outcome which may be important to Cyberdome based on its priority, criticality, usefulness, requirement and effectiveness. The work is evaluated by the Cyberdome team and reported to the Nodal Officer. The approval to count the work as a quantifiable one is the sole discretion of the Operations Officer and Nodal Officer.

*All Volunteers should submit a Self- assessment document annually based on their contributions to Cyberdome/Department/the Society/ Public/ their concerned which will be reviewed by the Cyberdome authority.



3.Off Boarding Process

Title	Exit Criteria	Off- boarding - Employee Requirements		Checklist
		Things to be returned	Agreements	
Information Security Advisor	On request for discontinuance/ Violation of organisational policies/ unproductive.	All devices/gadgets/documents issued if any. ID card/ Security cards/keys/Tools.	Non-Disclosure Agreement Cyberdome Volunteer Agreement	1. Revoke system access 2. Remove access entry 3. Change passwords and other access codes 4. Collect organisations assets 5. Redirect emails and calls 6. Remove from official Media groups
Commander/Cyberdome Project Governing Council Members	On request for discontinuance/ Violation of organisational policies/ Unproductive.	All devices/gadgets/documents issued if any. ID card/ Security cards/keys/Tools.	Non-Disclosure Agreement Cyberdome Volunteer Agreement	1. Revoke system access 2. Remove access entry 3. Change passwords and other access codes 4. Collect organisations assets 5. Redirect emails and calls 6. Remove from official Media groups
Deputy Commander		All devices/gadgets/documents issued if any. ID card/ Security cards/keys/Tools.	Non-Disclosure Agreement Cyberdome Volunteer Agreement	
Assistant Commander		All devices/gadgets/documents issued if any. ID card/ Security cards/keys/Tools.	Non-Disclosure Agreement Cyberdome Volunteer Agreement	

Junior Commander	On request for discontinuance/ Violation of organisational policies/ Unproductive.	All devices/gadgets/documents issued if any. ID card/ Security cards/keys/Tools.	Non-Disclosure Agreement Cyberdome Volunteer Agreement	1. Revoke system access 2. Remove access entry 3. Change passwords and other access codes 4. Collect organisations assets 5. Redirect emails and calls 6. Remove from official Media groups
R&D Associate		All devices/gadgets/documents issued if any. ID card/ Security cards/keys/Tools.	Non-Disclosure Agreement Cyberdome Volunteer Agreement	
Elite Member		All devices/gadgets/documents issued if any. ID card/ Security cards/keys/Tools.	Non-Disclosure Agreement Cyberdome Volunteer Agreement	
Volunteer		All devices/gadgets/documents issued if any. ID card/ Security cards/keys/Tools.	Non-Disclosure Agreement Cyberdome Volunteer Agreement	
Project Student/Trainee/ Associate		All devices/gadgets/documents issued if any. ID card/ Security cards/keys/Tools.	Non-Disclosure Agreement Cyberdome Volunteer Agreement	

4.Code of Conduct for Volunteers

i. Policy brief & purpose

This Code of Conduct for Volunteers policy outlines Cyberdome's expectations regarding volunteers' behaviour towards their team members, supervisors and to the overall organization. Cyberdome respect freedom of expression and open communication. But we expect all Cyberdome volunteers to follow this code of conduct policy. Volunteers should avoid offending, participating in serious disputes and disrupting in Cyberdome's workplace (Workplace may be physical or virtual office). Cyberdome also expect volunteers to foster a well-organized, respectful and collaborative environment. It is mandatory to always act with fairness, honesty, integrity and openness; respect the opinions of others and treat all with equality and dignity without regard to gender, race, colour, creed, ancestry, place of origin, political beliefs, religion, marital status, disability, age, or sexual orientation. Since strict observance of the Code of Conduct for Volunteers is fundamental to the activity and reputation of the Cyberdome, management has the responsibility of ensuring compliance with Code of Conduct for Volunteers.

ii. Scope

This policy applies to all users of Kerala Police Cyberdome resources/assets. All employees, contractors, consultants, volunteers/commanders/Interns, any individual/partner/partner organization associating with Kerala Police Cyberdome, temporary and other workers at Kerala Police Cyberdome, including all personnel affiliated with third parties must adhere to this policy. All Volunteers/other associates of Cyberdome are bound by their contract to follow our Code of Conduct while performing their duties and while associating with the Cyberdome.

iii. Compliance with law

All must protect our organisation's legality. They should comply with all environmental, safety and fair dealing laws. Cyberdome expects all its associates to be ethical and responsible when dealing with organisation's activities, collaboration, products, partnerships and public image.

iv. Respect in the workplace

All should respect their colleagues. Cyberdome won't allow any kind of discriminatory behaviour, harassment or victimization. Everyone should conform with equal opportunity policy in all aspects of their work, from recruitment and performance evaluation to interpersonal relations.

v. Protection of organisational Property

All should treat our organisation's property, whether material or intangible, with respect and care. Volunteers/commanders/other associates/partners:

- Shouldn't misuse **company equipment** or use it frivolously.
- Should respect all kinds of **incorporeal property**. This includes trademarks, copyright and other property (information, reports etc.).All should use them only to complete their job duties/responsibilities.
- All should protect company facilities and other material property from damage and vandalism whenever possible.

vi. Professionalism

All volunteers must show integrity and professionalism in their work and workplace. Act with fairness and honesty in all your dealings — be objective and transaction-oriented.

vii. Job duties and authority

All volunteers should fulfil their job duties with integrity and respect toward public, stakeholders and the community. Cyberdome expects team members to follow team leaders'/supervisors' instructions and complete their duties with skill and in a timely manner.

viii. Conflict of interest

All volunteers are expected to avoid situations in which his or her financial or other personal interests or dealings are, or may be, in conflict with the interests of the Cyberdome. Accordingly, the Cyberdome expects its volunteers to act in the Cyberdome's interest at all times. Cyberdome expects everyone to avoid any personal, financial or other interests that might hinder their capability or willingness to perform their job duties. Volunteers must not

use any Cyberdome's property, information or position, or opportunities arising from these for personal gains or to compete with or to tarnish the image of the Company. All Volunteers must avoid situations in which their personal interest could conflict with the interest of the Cyberdome. If, under any circumstance, Volunteers' personal interests conflict with those of the Cyberdome's, in all such cases the volunteers must seek advice from his or her reporting/ reviewing manager/supervisor or from Cyberdome management.

ix. Collaboration

Volunteers should be friendly and collaborative. They should try not to disrupt the workplace or present obstacles to their colleagues' work.

x. Communication

All must be open for communication with their peers, supervisors or team members.

xi. Utilization of Benefits

We expect volunteers to not abuse/misuse their benefits offered by Cyberdome. The benefits can be referred to any facilities, subscriptions, ID Cards, conveyance, internet or any other benefits Cyberdome offers.

xii. Policies

All volunteers should read and follow all Cyberdome policies. If they have any questions, they should ask their managers or Human Resources (HR) section of the Cyberdome.

5.Media Policy

i. Policy brief & purpose

Cyberdome Media policy establishes a set of standard expectations regarding volunteers' behaviour when using/interacting with all types of media. It sets out how volunteers/other associates must behave when interacting on media on behalf of Cyberdome. It also explains the rules about using personal social media accounts and describes what Cyberdome Employees/Volunteers/other associates may say about the organisation on their personal accounts. This policy should be read alongside other key policies. The organisations internet use policy is particularly relevant to staff using social media. This policy applies to professional and personal use of social media by Employees/Volunteers/other associates who undertake paid or voluntary work on behalf of the Cyberdome

ii. Purpose

Media can bring significant benefits to Cyberdome, particularly for reaching out to the general public. However, it's important that everyone who interacts with media on behalf of Cyberdome do so in a way that enhances the organisations prospects. A misjudged statement can generate complaints or damage to the organisation's reputation. This policy and its supporting guidance aim to:

- Support appropriate use of social media for personal and professional purposes.
- Clarify the boundaries between Cyberdome-related and private use of social media.
- Safeguard the interests and privacy of stockholders and staff Cyberdome as well as retain their trust.
- Promote security and privacy online.
- Maintain the security of IT systems and infrastructure of Cyberdome.
- Protect intellectual property rights, information assets, financial interests and competitive edge of Cyberdome.
- Maintain reputation and integrity of Cyberdome as well as to comply with the law of land.

- Confirm what is acceptable and what is unacceptable behaviour in terms of social media usage is.

iii. Policy scope

iv. This policy applies to all users of Kerala Police Cyberdome resources/assets. All employees, contractors, consultants, volunteers/commanders/Interns, any individual/partner/partner organization associating with Kerala Police Cyberdome, temporary and other workers at Kerala Police Cyberdome, including all personnel affiliated with third parties must adhere to this policy. All Volunteers/other associates of Cyberdome are bound by their contract to follow our Code of Conduct while performing their duties and while associating with the Cyberdome. This policy applies to any communications made on behalf of Cyberdome/dealing with any kind information relating to Cyberdome to any kind of media at any time and from anywhere. This policy applies to all Volunteers/Commanders/ other associates at Cyberdome on how their interactions must be with all medias; visual/printed/other media— no matter whether for official or personal reasons. Media and services include (but are not limited to):

a. All visual or printed Medias.
b. Popular social networks.
c. Messenger applications.
d. Online review websites.
e. Sharing and discussion sites.
f. Photographic social networks.
g. Question and answer social networks.
h. Professional social networks.

v. Interactions with mass media (visual/printed/any other media)

Cyberdome volunteers/Commanders/other associates are not permitted to interact with mass Medias in any manner on behalf of Cyberdome unless otherwise specifically authorised by the Cyberdome authority. In such cases of specific authorisation a written permission must be obtained from the Cyberdome authority before interacting with mass media on behalf of Cyberdome. Cyberdome volunteers/Commanders/other associates must not mention their honorary ranks they have in Cyberdome while interacting with mass media if they are doing so

in their personal interests. When interacting with mass media on behalf of Cyberdome, volunteers/Commanders/other associates must use good judgement about what they say and about the appropriateness of statements since a misjudged statement can have a heavy toll on the reputation of the organisation.

vi. Creating social media accounts

New social media accounts in the organisation's name must not be created unless approved by the Cyberdome authority. Cyberdome operates its social media presence in line with a strategy that focuses on the most-appropriate social networks, given available resources. If there is a case to be made for opening a new account, it should raise with the Operations Officer, Cyberdome.

vii. Inappropriate content and uses

Cyberdome social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the organisation into disrepute. When sharing an interesting blog post, article or piece of content, all should always review the content thoroughly, and should not post a link based solely on a headline.

viii. Talking about the organisation

a. Volunteers/other associates should ensure it clear that their social media account does not represent Cyberdome's views or opinions.
b. Include a disclaimer in social media profiles: 'the views expressed are my own and do not reflect the views of Cyberdome.'
c. Use good judgment about what you post and remember that anything you say can reflect on Cyberdome even if you do include a disclaimer. Always strive to be accurate in your communications about Cyberdome and remember that your statements have the potential to result in liability for yourself or Cyberdome. Be respectful to Cyberdome and be professional and honest in your communications.

d. Volunteers/other associates should use their best judgment in posting material that is either inappropriate or harmful to Cyberdome, its employees, or individuals. If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication.
e. Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Volunteers/other associates should refer these inquiries to the Cyberdome authority.
f. If you see content in social media that disparages or reflects poorly on Cyberdome or its stakeholders, you should contact Cyberdome. Protecting Cyberdome's goodwill, brands and reputation is every volunteer's responsibility.

ix. Respect Intellectual Property and Confidential Information

Cyberdome restricts Volunteers/other associates use and disclosure of the organisations confidential information and intellectual property. Beyond these mandatory restrictions, you should treat the organisations valuable secrets and other confidential information and intellectual property accordingly and not do anything to jeopardize them through your use of social media. If there are questions about what is considered confidential, Volunteers/other associates should check with Cyberdome authority. In addition, you should avoid:

- Misappropriating or infringing the intellectual property of other organisations and individuals, which can create liability for you and for Cyberdome.
- Do not use Cyberdome's logos, brand names, taglines, slogans or other trademarks, or post any confidential or proprietary information of the organisation, without prior permission from the Cyberdome authority.

x. Safe and Responsible Social Media Use

The rules in this section apply to any Volunteers/other associates using Cyberdome social media accounts. Users must not:

a. Create or transmit material that might be defamatory or incur liability for the organisation.

b. Post message, status updates or links to material or content that is inappropriate. Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.
c. This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
d. However, this doesn't restrict volunteers from sharing such things as part reporting such incidents to the Cyberdome. In that case Volunteers are free to report provided the same must be done only through Personal Messages to the group admins or through Cyberdome official e-mail/website.
e. Use social media for any illegal or criminal activities.
f. Send offensive or harassing material to others via social media.
g. Broadcast unsolicited views on social, political, religious or other non-business related matters.
h. Send or post messages or material that could damage Cyberdome's image or reputation.
i. Post, upload, forward or link to spam, junk email or chain emails and messages.
j. Mention their honorary title at Cyberdome in their social media accounts without explicitly mentioning as honorary.
k. Make any statement or respond to any query/comment on behalf of Cyberdome without email approval from the Cyberdome authority

xi. Copyright

Cyberdome respects and operates within copyright laws. Users may not use social media to:

a. Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
b. Share links to illegal copies of music, films, games or other software.

xii. Security and Data Protection

Employees/Volunteers/other associates should be aware of the security and data protection issues that can arise from using social networks.

xiii. Maintain Confidentiality

Employees/Volunteers/other associates must not:

a. Share or link to any content or information owned by Cyberdome that could be considered confidential or sensitive.
b. Share or link to data in any way that could breach Cyberdome's data protection policy.

xiv. Policy enforcement

a. Monitoring social media use - Company IT and internet resources — including computers, smart phones and internet connections — are provided for legitimate use.
b. The organisation therefore reserves the right to monitor how social networks are used and accessed through these resources.
c. Any such examinations or monitoring will only be carried out by authorised staff.
d. Additionally, all data relating to social networks written, sent or received through the organisations computer systems is part of official records.
e. Cyberdome can be legally compelled to show that information to law enforcement agencies or other parties.

xv. Potential sanctions

Knowingly breaching this Media Policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including legal action. Volunteers, Commanders and other users may also be held personally liable for violating this policy. Activities that violate Cyberdome's Information Security Policies or any other Organizational policy may subject Employees/Volunteers/other associates to disciplinary action or termination. Where appropriate, the organisation will involve the law enforcement agencies in relation to breaches of this policy.

6.Disciplinary Actions

i. Policy brief & purpose

Cyberdome may have to take disciplinary action against volunteers who repeatedly or intentionally fail to follow Cyberdome's volunteer code of conduct or any Cyberdome policy. Disciplinary actions will vary depending on the violation. This Disciplinary action policy explains how Cyberdome addresses its volunteers' misconduct or inappropriate performance.

ii. Purpose

Purpose of this document is to make Cyberdome volunteers to make aware of the consequences of their inappropriate actions while working with Cyberdome. This policy outlines Cyberdome's disciplinary procedures against volunteers on their misconduct to the Organization.

iii. Scope

This policy applies to all users of Kerala Police Cyberdome resources/assets. All employees, contractors, consultants, volunteers/commanders/Interns, any individual/partner/partner organization associating with Kerala Police Cyberdome, temporary and other workers at Kerala Police Cyberdome, including all personnel affiliated with third parties must adhere to this policy. All Volunteers/other associates of Cyberdome are bound by their contract to follow our Code of Conduct while performing their duties and while associating with the Cyberdome. This policy applies to any communications made on behalf of Cyberdome/dealing with any kind information relating to Cyberdome to any kind of media at any time and from anywhere. This policy applies to all Volunteers/Commanders/ other associates at Cyberdome on how their interactions must be with all medias; visual/printed/other media— no matter whether for official or personal reasons

iv. Policy Elements

The stages that may be followed when discipline is deemed necessary include the following:

1. Verbal warning
2. Corrective Actions
3. Official reprimand
4. Disciplinary meeting with appropriate supervisory authority
5. Final written warning
6. Detraction of benefits
7. Indefinite suspension or demotion
8. Termination
9. Legal action in cases of corruption, theft, embezzlement or other unlawful behaviour

The nature of the offense must be explained to the volunteer from the beginning of the procedure. The verbal warning may take the form of a simple oral reprimand but also a full discussion if that is necessary. The volunteer must read and sign the written reprimand and final written warning. These documents include the time limit in which a volunteer must correct their conduct before we take further disciplinary action.

The following scenarios indicate where the disciplinary procedure starts depending on the violation:

- Misdemeanours/One-time minor offense: Disciplinary procedure starts at stage 1. It includes but is not limited to:
  1. Rude behaviour to the organisation members or partners.
  2. On-the-duty minor mistakes.
  3. Inappropriate use of Cyberdome proprietary materials.

4. Violation of Cyberdome Policies

- Misconduct/Frequent offender. Disciplinary procedure starts at stage 5. It includes but is not limited to:
  1. Lack of response to corrective actions.
  2. Frequent Inappropriate use of Cyberdome Proprietary materials.
- Severe offensive behaviour/Felony: Disciplinary procedure starts at stage 6. It includes but is not limited to:
  1. Corruption/ Bribery.
  2. Breach of Cyberdome policies/agreements.
  3. Harassment/ Voluntary discrimination.
  4. Workplace Violence.
  5. Embezzlement/Fraud.

Cyberdome Operation Officer / Nodal Officer / Management / HR team may choose to repeat stages of our disciplinary procedure as appropriate. This decision depends on volunteers' reaction to our disciplinary procedure, whether they repent their behaviour and the nature of their offense. Our disciplinary procedure begins when there is sufficient evidence to justify it. When there is suspicion or hints of misconduct, managers or HR must investigate the matter first. We are obliged to refrain from disciplinary actions that may constitute retaliatory behaviour. We have the right to modify this policy or act in any other legal or reasonable way as each case demands. But, we will always enforce discipline in a fair and lawful manner.