GSMA Coordinated Vulnerability Disclosure Program

Version 3.0

16 July 2020

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

Coordinated Vulnerability Disclosure (CVD) of security vulnerabilities is a well-established process which allows people or groups, such as security researchers, to report details of security vulnerabilities in products and services. The GSMA CVD programme provides a framework that sets clear expectations for constructive engagement by all parties to remediate or mitigate notified vulnerabilities.

The early disclosure of vulnerabilities can help to protect end users, allowing manufacturers and providers of products and services to address security issues before public disclosures are made.

The GSMA operates a programme for CVD ("CVD Programme") to better protect mobile industry systems, mobile users and the wider industry ecosystem. The GSMA's CVD Programme does not consider vulnerabilities affecting an individual manufacturer or operator, but deals with security vulnerabilities that impact the mobile industry as a whole. This means that vulnerabilities which are non-manufacturer specific can be reported, remediation options considered and actioned.

This document, and its associated components, has been built around best practice recommendations contained in ISO/IEC 27001:2013 [1] and ISO/IEC 29147:2018 [2] pertaining to the handling and communication of disclosures, and The CERT® Guide to Coordinated Vulnerability Disclosure [3][3]. Because GSMA's CVD Programme is pan-industry, it does not align with all aspects within these recommendations, which focus on programmes run by individual manufacturers or providers of services.

1.2 Definition of Terms

Term	Description
Activity	Any activity undertaken by an Association's project, forum, task force or any other group constituted in accordance with the Articles of Association.
Coordinator	An individual or organisation that performs a set of activities including identifying and engaging stakeholders, mediating, communicating, and other planning in support of vulnerability disclosure. The CVD Director takes on this role in the GSMA CVD Programme.
CVD Director	The director of the CVD Programme as appointed by the GSMA.
Exploit	A technique that takes advantage of a security vulnerability to cause unintended or unanticipated behaviour to occur.
Fraud and Security Architecture Group	The subgroup of the GSMA's Fraud and Security Group that is focussed on the protection of networks and smart cards, and engagement with researchers to realise improved security levels.
Fraud and Security Group [10]	The GSMA's Group which leads the mobile industry's management of fraud and security matters related to mobile technology, networks and services, with the objective to maintain or increase the protection of mobile operator technology and infrastructure, customer identity, security and privacy such that consumers are protected from harm, the industry's

Term	Description
	reputation stays strong and mobile operators remain trusted partners in the ecosystem.
GSMA Members, Associate Members and Rapporteurs	Members, Associate Members or Rapporteurs of the GSMA in accordance with the articles of association and regulations governing the GSMA.
Incident	One or multiple related and identified occurrences indicating a possible breach of information security or failure of controls that can harm an organisation's assets or compromise its operations.
Manufacturer	The individual or organisation that develops a product or service or is responsible for its maintenance. This includes an individual or organisation such as a commercial business or an organisation that delivers software or services for free.
Minimum viable details	The minimum information about a vulnerability as is required to satisfy the legal or regulatory notification requirement. This is considered to be information required to prevent an Incident from occurring rather than revealing information about the vulnerability.
Mitigation	A workaround or countermeasure that eliminates, or reduces the likelihood or impact of a successful attack.
Panel of Experts	The group of experts from GSMA Members, Associate Members and Rapporteurs who consider Submissions in their area of expertise, and review the GSMA CVD Programme.
Remediation	A change made to a product or service to remove or mitigate a vulnerability.
Reporter	An individual or organisation that notifies a manufacturer or Coordinator of a potential vulnerability.
Submission	The information about a vulnerability that is provided to the GSMA CVD by a Reporter.
Submission Consideration Group	A group convened by GSMA to consider a specific Submission made up of the Panel of Experts, Submission Specific Experts and GSMA staff.
Submission Specific Expert	An expert in a particular area invited by the GSMA to consider a specific CVD Submission as part of the Submission Consideration Group. They may or may not be affiliated with GSMA Members, Associate Members and Rapporteurs.
User	A user of a product or service, who may also be referred to as customers, consumers or end users.
Vulnerability	The functional behaviour of a product or service that violates an implicit or explicit security policy.
Vulnerability Disclosure	The act of initially providing vulnerability information to a party that was not believed to be previously aware.

1.3 Abbreviations

Term	Description
CVD	Coordinated Vulnerability Disclosure

Term	Description
FASG	Fraud and Security Group
FSAG	Fraud and Security Architecture Group
GPG	GNU Privacy Guard
ISO	International Standards Organisation
POC	Proof of Concept
PoE	Panel of Experts
SCG	Submission Consideration Group

1.4 References

Ref	Title	Link
[1]	ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements	https://www.iso.org/standard/54534.html
[2]	ISO/IEC 29147:2018 Information Technology – Security Techniques – Vulnerability Disclosure	https://www.iso.org/standard/72311.html
[3]	The CERT Guide to Coordinated Vulnerability Disclosure	https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf
[4]	GSMA CVD webpages	http://www.gsma.com/cvd/
[5]	GSMA Security.txt	https://www.gsma.com/.well-known/security.txt
[6]	Mobile Security Research Hall of Fame	https://www.gsma.com/security/gsma-mobile-security-hall-of-fame/
[7]	CVD on InfoCentre[2]	https://infocentre2.gsma.com/gp/wg/FSG/CVD/Pages/Default.aspx
[8]	GSMA AA.16	https://www.gsma.com/aboutus/wp-content/uploads/2019/08/AA.16-v3.19.pdf
[9]	GSMA Antitrust Policy Statement	https://www.gsma.com/aboutus/legal/anti-trust-policy-statement
[10]	Fraud and Security Group	https://www.gsma.com/aboutus/workinggroups/fraud-security-group

2 GSMA CVD Policy

Through its CVD programme the GSMA aims to cooperate with vulnerability Reporters and security researchers to better protect mobile industry systems, mobile users and the wider industry ecosystem.

2.1 Scope of the GSMA CVD Programme

2.1.1 In Scope

The scope of the CVD Programme is security vulnerabilities that impact the mobile industry, primarily open standards based technologies.

2.1.2 Out of Scope

The following items are out of scope for the CVD Programme.

- Research or information on a vulnerability which has previously been made public. Research or information on a vulnerability which is already in the public domain is out of scope for inclusion in the Hall of Fame, but may be considered through the CVD Programme in order to develop remediations.
- Services or products provided by a single Manufacturer or Manufacturer group, these should be reported to the relevant Manufacturer.
- Services or products provided by a single company or group of companies. These should be reported to the relevant company.
- Submissions by GSMA Members, Associate Members and Rapporteurs where they are working on the topic as part of an Activity. These should be reported through the relevant Activity.

Vulnerabilities in GSMA websites or services – should be reported to webmaster@gsma.com.

2.2 Reporting a vulnerability to the GSMA

To make a Submission, Reporters are requested to complete one of the templates found at www.gsma.com/cvd [4] and email it to security@gsma.com. GPG encryption is encouraged but not required, the public key can be found at [4].

Further information is available at www.gsma.com/.well-known/security.txt [5].

During the process, communication with the GSMA is requested to be in English, by email and through a single main Reporter (Section 5.1 contains more information).

2.2.1 Timings

The GSMA aims to:

- Acknowledge a Reporter's Submission within 2 working days of receiving a completed Submission form.

- Make an initial appraisal of the Submission, and provide a response within 10 working days of receiving a completed Submission form.

Depending on the nature of the vulnerability the timescale for remediation will vary; the default for the GSMA's response is 90 days. This will be discussed with the Reporter to manage expectations.

GSMA does not carry out remediation in networks or equipment on behalf of individual companies, and is not empowered to make changes to standards defined by external bodies. This remediation work will require additional time, after the steps laid out in Section 5, and will vary between companies.

2.3 Disclosure

The GSMA's timeline for remediation and public disclosure will be determined by the vulnerability, the route(s) to remediation, and the scale of remediating actions. The GSMA will also consider external deadlines the Reporter has committed to such as publications or conferences.

To assist with coordination, the GSMA requests that Reporters confirm to which other organisations they have disclosed the vulnerability.

The GSMA will consider whether other organisations are required to carry out remediating actions. When required, the GSMA will confirm the Reporter is happy for this discussion to occur, and whether the Reporter wishes to be named in these communications.

As part of the consideration and remediation of a vulnerability, the GSMA may create advisories and outputs for the benefit of the mobile industry, such as a briefing papers and statements relating to the vulnerability. These will be shared with the GSMA Members, Associate Members and Rapporteurs under a confidentiality notice.

2.4 Credit to Reporter

If appropriate and acceptable to the Reporter, the GSMA will recognise disclosures by naming the Reporters in its publicly hosted "Mobile Security Research Hall of Fame" [6].

Entry to the Mobile Security Research Hall of Fame is determined by the GSMA on a case-by-case basis. The eligibility criteria for the Mobile Security Research Hall of Fame are found in Section 5.7.1.

2.5 Research Expectations

The GSMA is grateful to Reporters who afford us the opportunity to consider their findings, liaise with the industry and define remediation and mitigation actions.

However, participation in the CVD Programme requires that Reporters do not engage in activities that violate any local legislation or regulations and third party rights.

Reporters are asked to:

1. Not abuse the reported vulnerability. For example, downloading more data than is necessary to demonstrate the vulnerability, or changing/deleting live systems, settings or data.

2. Exercise caution and restraint with regard to personal data and not intentionally engaging in attacks against third parties, social engineering, denial-of-service attacks, spamming or otherwise causing a nuisance to other users.

If there is any doubt, please contact security@gsma.com.

3 General

3.1 Document scope

This document outlines the policy, process and functions relating to the GSMA CVD Programme; setting clear expectations for anybody engaging with the process.

3.2 Programme Goals

The GSMA CVD Programme is built around one central goal:

- Protect the mobile telecommunications industry, and consumers, by considering and managing options available to remediate vulnerabilities affecting mobile telecommunications before they are disclosed publicly.

To enable this, the Programme's sub-goals are to:

1. Handle reported vulnerabilities in a coordinated manner with the necessary expertise.
2. Protect the confidentiality and integrity of the process, and submitted research, in order to retain the confidence of the GSMA CVD Programme.
3. Protect all parties in the process from actual or perceived conflicts of interest.

To achieve these goals the GSMA rely on a specialist group, who use their knowledge to assess a Submission and consider options for remediation; the Panel of Experts (PoE) (Section 4).

4 The Panel of Experts

The PoE is a subject matter expert group drawn from individuals working for GSMA Members, Associate Members and Rapporteurs. This group supports the GSMA deal with security vulnerabilities submitted to the CVD Programme. Members are chosen by the GSMA based on their personal skills, capabilities and ability to commit to the Programme.

PoE members commit to work for the benefit of the industry as a whole, rather than to enable competitive advantage.

Non-GSMA Members, Associate Members and Rapporteurs' employees or personnel may be invited on a case by case basis to participate as a Submission Specific Expert.

4.1 Make-up of the Panel of Experts

Alongside a general security mind-set, the GSMA has identified the following areas of experience and expertise as required for the PoE to collectively have:

- Transport/transmission security
- Radio access network (RAN) security
- Signalling protocol security
- Core network technology security
- Device security
- UICC/eUICC security
- Cryptography
- Internet of Things (IoT) security
- Roaming and interworking security
- Cloud and virtualisation security
- Billing and financial system security
- Protocol analysis/security

It is desirable that each area should be represented by at least two individuals on the PoE.

It would be undesirable for a company or geographic region to be overrepresented on the PoE. The GSMA aims to have:

- A maximum of two PoE members working for the same organisation, unless additional members are covering areas of expertise that would otherwise not be sufficiently represented.
- Representation from a range of geographic regions.

The GSMA FASG Chair is a member of the PoE for the duration of their chairmanship by virtue of holding the position.

4.2 Joining the Panel of Experts

Individuals working for GSMA Members, Associate Members and Rapporteurs are eligible to join the PoE.

To apply, applicants should complete the application form found at [4] and send it to cvd@gsma.com. GPG encryption is encouraged but not required, the public key can be found at [4].

In order to join the PoE, it is the responsibility of the individuals to:

1. Be recognised by the telecommunications industry or academic community as specialists in a relevant area of mobile telecommunications security

2. Be active contributors to the community in their chosen area of research or expertise

3. Align with GSMA's organisational objectives and values

Biannually the GSMA will consider all complete applications submitted by the required deadline to the nominated email. The GSMA will assess individuals' applications based on the requirements in this section and Sections 6.3 and 6.4 of this document.

The current application deadline is provided at [4].

To allow outgoing members of the PoE to attend the CVD Annual Review meeting in April, the application process will begin after this date by announcement to the FASG.

The decision to appoint an individual to the PoE sits with the GSMA. The route of appeal against the decision not to accept an applicant to the POE is via the GSMA CTO (CTO_Office@gsma.com). The appeal must be entered within 5 working days of the applicant being notified of the GSMA's decision.

Figure 1 summarises the application process, along with anticipated timelines for the application process.

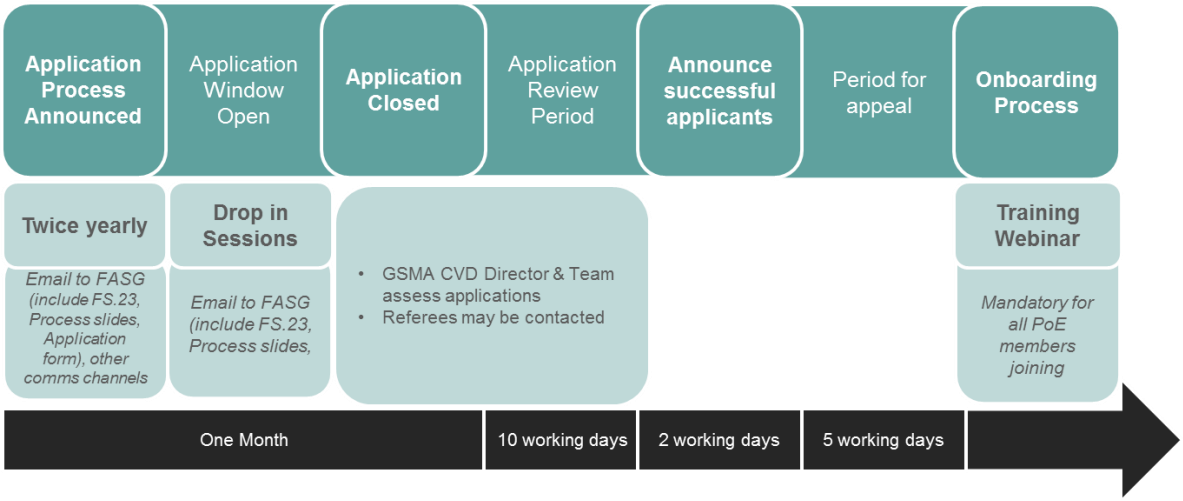

Figure 1: PoE application process

4.3 Period of appointment and removal from the Panel of Experts

PoE members are appointed for two years from the date of their official confirmation of participation by the GSMA, with the ability to re-apply. Should members of the PoE wish to remain past their two year term, the individual is expected to reapply using the process in Section 4.2. If no application is received the PoE member's term will automatically end after two years.

The GSMA will remind PoE members that their term is due to expire, with sufficient time for the PoE member to reapply.

If a PoE member stops working for one of the GSMA Members, Associate Members and Rapporteurs, their appointment to the PoE will lapse, unless they are able to demonstrate that they will begin to work for another of the GSMA Members, Associate Members and Rapporteurs within three months.

PoE members may resign at any time by writing to the CVD Director. This will not alter the application process timeline (see 4.2).

If a PoE member does not meet the responsibilities listed under Sections 4.2, 6.3 and 6.4 of this document their appointment to the PoE will be reviewed by GSMA which may result in the member being removed from the PoE.

The route of appeal against the removal from the PoE is via the GSMA CTO (CTO_Office@gsma.com). The appeal must be entered within 5 working days of the applicant being notified of removal.

5 CVD Submission and Consideration Process

5.1 Submission by Reporter

To submit a vulnerability to the GSMA CVD Programme, the Reporter should describe it in either of the Submission forms available in Annexes B.1 and B.2, also available online at [4], and email the completed form to security@gsma.com. GPG encryption is encouraged but not required, the public key can be found at [4].

The Reporter is requested to describe the vulnerability on the Submission form, including:

- Identification of the vulnerable target(s)
- A description of the vulnerability
- Operations carried out to exploit the vulnerability

This is usually sufficient information to enable the GSMA to consider the vulnerability and will allow for verification and identification of possible remediations. A Proof-of-Concept (POC) or more detailed description may be requested in the case of complex vulnerabilities.

The GSMA may ask a Reporter for more information throughout the consideration process.

Reporters agree to:

1. Submit information about vulnerabilities using either of the Submission forms
2. Provide sufficient information in English to enable the GSMA to consider the Submission
4. Remain actively engaged with the GSMA throughout the consideration process through one main Reporter
5. Not publicise information about the vulnerability until it has been resolved within the agreed period, with a default of 90 days
6. Adhere to the expectations in Section 2.5

5.2 Validation and acknowledgement of a Submission

The GSMA aims to contact the Reporter within 2 working days of receipt of the Submission to thank the Reporter and:

- Where key information is not included on the Submission form, to ask for the missing information to be added and resubmitted

- Where the Submission form is complete, inform the Reporter of the consideration process and that it has been sent to the Submission Consideration Group (SCG)

In the case that a Reporter names specific GSMA Members, Associate Members and Rapporteurs being actively exploited using the vulnerability then the CVD process will define this as an Incident. In addition to the CVD process the CVD Director will contact the named

party to provide information about the incident, and if feasible may attempt to identify other (not already named) parties that may also be impacted.

5.3 Formation of a Submission Consideration Group and consideration of a Submission

Upon receiving a Submission the GSMA will invite the PoE and (on a need-to-know basis) any additional Submission-Specific Experts or GSMA staff to consider a Submission, forming a SCG for that specific Submission.

The SCG will decide if a reported vulnerability is admissible to the GSMA's CVD Programme based on the scope in Section 2.1 of this document.

They may ask for further information from the Reporter to help their consideration.

5.4 Informing the Reporter of the SCG's decision

The GSMA will inform the Reporter whether the submitted vulnerability has been accepted, deemed unsuitable for GSMA CVD, or if the SCG would like more information to reach a decision.

If it is deemed unsuitable for GSMA CVD, the GSMA will discuss with the Reporter the SCG's reasoning and provide this.

GSMA aims for this to take place within 10 working days from the GSMA's confirmation that the Submission form is complete and has been shared with the SCG. Regardless of acceptance, the GSMA will assign the Submission a CVD number (*CVD-YEAR-nnnn*) and provide it to the Reporter.

During the consideration of a Submission a member of the SCG may become aware of an Incident which a law, regulation or contract requires them to report. Under these circumstances the SCG member agrees to limit the information shared to Minimum viable details of the incident.

5.5 Remediation, including creation of advisories and outputs

To assist with coordination, the GSMA requests that Reporters confirm to which other organisations they have disclosed the vulnerability.

The GSMA will consider whether other organisations are required to carry out remediating actions. When required the GSMA will confirm the Reporter is happy for this discussion to occur, and whether the Reporter wishes to be named in these communications.

As part of the consideration and remediation of a vulnerability, the GSMA may create advisories and outputs for the benefit of the mobile industry; such as a briefing paper or statement relating to the vulnerability. These will be shared with GSMA Members, Associate Members and Rapporteurs under a confidentiality notice.

The Reporter and SCG will contribute to drafting these documents. Interim publication of advisories, briefings or other disseminations to GSMA Members, Associate Members and Rapporteurs will be considered on a Submission-by-Submission basis.

What	When	For whom	Purpose
Briefing paper	Prior to public disclosure	GSMA Members, Associate Members and Rapporteurs	To inform GSMA Members, Associate Members and Rapporteurs of the details and remediation routes for a submitted vulnerability
Reactive media statement	Ready for public disclosure or briefing paper dissemination	Inbound media enquiries	To respond to inbound media enquiries about a submitted vulnerability
Liaison Statement	At any point during consideration	Standards bodies responsible for an impacted standard	To inform other organisations of the information required to make a change to a standard to remediate a submitted vulnerability

Table 1: Typical outputs created by SCG

5.6 Ongoing communication

Ongoing communication and expectation management is a key aspect of CVD programmes. Setting communication and resolution expectations creates a culture of trust and provides credibility between GSMA and the Reporter. The timescale will vary between Submissions but the default is 90 days.

There will be ongoing communication between the GSMA and the Reporter, allowing the SCG to request further information or provide feedback to the Reporter. In turn, the Reporter may update the GSMA on any developments.

Where the publication date has not been confirmed, this should be determined during these communications.

5.7 Closedown of Submission

The Submission is closed when:

- No GSMA action is considered necessary or appropriate in relation to a Submission deemed unsuitable for GSMA CVD, or
- When an advisory is disseminated in response to an accepted Submission

This is done in discussion with the Reporter.

Remediation of the residual threat from the vulnerability to the industry should be considered where practically possible.

The closedown template (Annex B.3) will be completed and made available for GSMA Members, Associate Members and Rapporteurs on the InfoCentre2 CVD group [7], along with any GSMA outputs, the Submission and the Submission form.

Final decisions regarding inclusion in the Mobile Security Research Hall of Fame [6] should be made at this point and the Reporter informed of the decision.

5.7.1 Mobile Security Research Hall of Fame

Entry into the Mobile Security Research Hall of Fame is based on the following criteria:

1. Meeting the scope for the CVD Programme (Section 2.15.3 of this document)
2. Impact of the vulnerability
3. Reporter's engagement with the process

The GSMA reserves the right to remove Reporters from the Mobile Security Research Hall of Fame if they no longer meet these criteria or subvert the mobile industry's security efforts.

EXAMPLE Attacks on live networks or other activities which undermine the confidentiality, availability or integrity of systems would constitute subversion of the mobile industry's security efforts.

5.8 Updating of Submission

When further information is provided about a Submission, either directly from the Reporter or from elsewhere (e.g. the press), the update is noted and provided to the SCG, ensuring the most comprehensive and up-to-date information is considered. This may result in updated advisories or outputs being published.

The GSMA monitors the internet for updates to the underlying research, as deemed appropriate by the PoE. Reporters and GSMA Members, Associate Members and Rapporteurs are also encouraged to provide GSMA with such updates.

5.9 Submission disputes

If a Reporter and the GSMA cannot reach an agreed position on a Submission it is recommended that further attempts are made to resolve the issue in a clear and open manner. Guidance should be provided to the Reporter as to what will happen should no further agreement be reached, or communication be received.

If the issues cannot be resolved, the discussion should be closed down in a manner that provides options to resume communications should the Reporter desire this at a later stage.

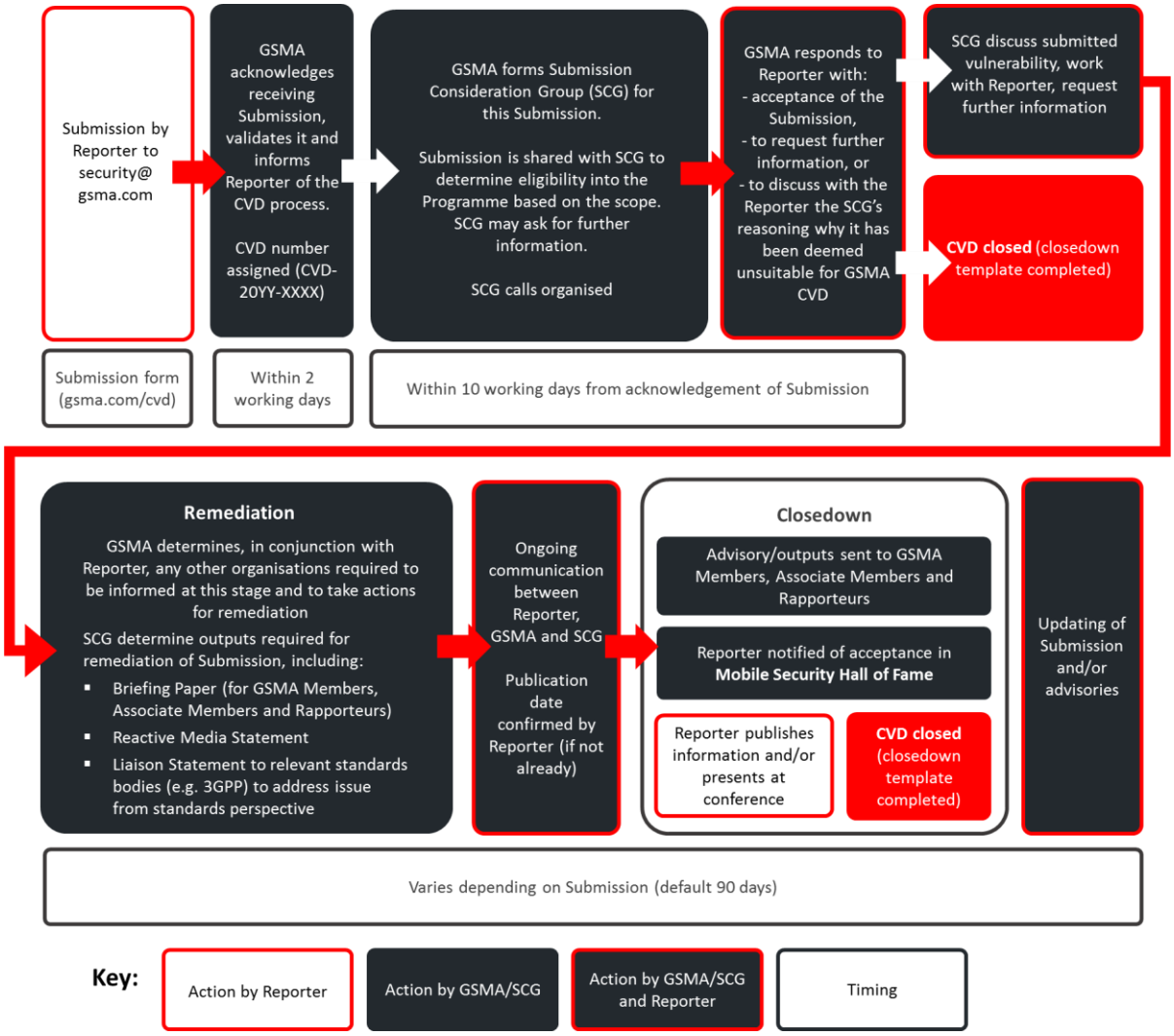

Figure 2: CVD Submission and Consideration Process workflow

6 Roles and Responsibilities

6.1 CVD Director Responsibilities

Role	Responsibilities
The CVD Director coordinates between the Reporter, the SCG, and others involved in the process; including relevant GSMA staff, GSMA Members, Associate Members and Rapporteurs, and other relevant organisations.	The CVD Director will: • Lead the day-to-day running of the Programme • Be the GSMA point of communication for a Reporter and the route of communication between the SCG and Reporter • Uphold the highest standards of ethics and integrity through their conduct both within and outside of the CVD process • Carry out the initial check of a Submission when it is received by the GSMA

Role	Responsibilities
	• Act as liaison to any GSMA staff function that needs to be involved in the Programme • Approach any Submission Specific Experts to join a SCG • Organise all meetings of the PoE and SCGs • Administer the PoE application process including deciding on new members to appoint to the PoE • Remove a PoE member who has not followed the responsibilities listed under Sections 4.2, 6.3 and 6.4 of this document • Administer the quarterly PoE conference calls and the CVD Programme Annual Review • Carry out all reporting as listed in Section 8 of this document

Table 2: CVD Director Role and Responsibilities

6.2 GSMA CTO Responsibilities

Role	Responsibilities
The GSMA CTO owns the GSMA CVD Programme.	The GSMA CTO will: • Act as the sole route of appeal for applicants to the PoE who are not appointed by the CVD Director • Act as the sole route of appeal for PoE members removed by the GSMA CVD Director • Support the long term funding of the Programme. This includes support services that are essential to the smooth running of the GSMA CVD Programme such as finance, legal and communications

Table 3: GSMA CTO Role and Responsibilities

6.3 Panel of Experts Member Responsibilities

Role	Responsibilities
The PoE consider and remediate a Submission as part of a SCG and provide expertise based on their individual skillsets and experience. The group also input to the Programme's overall strategic roadmap which is delivered through the GSMA.	As part of the PoE, it is the responsibility of members to: • Individually adhere to the GSMA's confidentiality requirements as per Article 18.2 of the GSMA Articles of Association (AA.16) [8]

Role	Responsibilities
	• Work for the benefit of the industry as a whole rather than to enable competitive advantage • Attend the GSMA's required training webinar when they are appointed, before taking part in Submission reviews • Be actively involved in regular meetings and contribute to work • Uphold the highest standards of ethics and integrity through their conduct both within and outside of the CVD process • Provide expertise on vulnerability disclosure management to support the GSMA's CVD Programme • Take part in the quarterly PoE conference calls and attend the Annual Review meeting, where organisational travel policy permits

Table 4: PoE Role and Responsibilities

6.4 Submission Consideration Group Responsibilities

Role	Responsibilities
This group's role is to consider the vulnerability, its implications, remediation options and the GSMA's response to a Submission, and to actively contribute to all material in Section 5.5. This includes admission of the Reporter to the Mobile Security Research Hall of Fame [6]. This group may consist of individuals not from GSMA Members, Associate Members and Rapporteurs, referred to as Submission Specific Experts, in addition to the PoE and GSMA staff.	It is the responsibility of SCG members to: • Assess the admissibility of vulnerabilities in accordance with the GSMA's eligibility criteria in Section 2.15.3 • Suggest appropriate Submission Specific Experts to the GSMA CVD Director to assist with the consideration of Submissions • Contribute to the formulation of the GSMA's response to each disclosure, see Section 5.5 • Inform the GSMA CVD Director when the Submission must be shared with others within their organisation • Agree to manage a list of who has had access to the information, to be provided to the GSMA in case of a suspected breach of confidentiality • Inform the GSMA CVD Director where they believe a breach of confidentiality may have occurred within their organisation • Notify the GSMA CVD Director of any potential or actual conflicts of interest when considering a Submission, in particular with

Role	Responsibilities
	relation to any disclosures required by law, regulation or contract • Not make contact with a Reporter directly during consideration of a Submission, unless authorised by the GSMA CVD Director In addition to points above Submission Specific Experts agree: • Where they do not work for GSMA Members, Associate Members and Rapporteurs, to sign and adhere to an individual GSMA NDA (Annex Annex C) covering their work on a Submission. • To adhere to the GSMA's confidentiality [8] and antitrust provisions [9] and not use shared Submissions for competitive advantage or to the disadvantage of the industry

Table 5: SCG Role and Responsibilities

7 Programme review

7.1 Quarterly Conference Call

The PoE holds a quarterly conference call to consider the status of Submissions received or closed within the preceding quarter, any media attention or any non-Submission specific matters. Communications of this nature may also take place by email.

7.2 CVD Programme Annual Review

The GSMA will hold an Annual Review meeting, usually in April, with the aim to continuously improve the Programme. All members of the PoE will be invited and topics for consideration may include:

- Submissions including number received and time taken to consider each Submission
- Feedback from Reporters and other parties
- Expertise gaps within the PoE for next application round consideration
- Suggestions for changes to the Programme

8 Reporting

The GSMA will report on the progress of individual Submissions and to understand the effectiveness of the Programme as a whole. GSMA groups may request ad hoc reports about the Programme.

8.1 Monthly reporting

The following will be reported to the PoE and to GSMA staff.

1. Number of Submissions:
    a) received that month
    b) deemed unsuitable for GSMA CVD that month
    c) currently under consideration
    d) closed that month (excluding deemed unsuitable for GSMA CVD)
2. The status of Submissions under consideration
3. Any Submissions which have not met the agreed timings for acknowledgement or initial assessment that month

The CVD Director may report other information or trends that they deem useful for the PoE, GSMA staff or others.

9 Disclosure and confidentiality

As part of the CVD Programme the GSMA will need to provide information about the Submission to GSMA Members, Associate Members, Rapporteurs and non-GSMA member Submission Specific Experts.

This information is shared with these groups on a need-to know basis and subject to the following confidentiality restrictions:

- The recipient of the information agrees to adhere to Article 18.2 of the GSMA Articles of Association (AA.16) [8].
- Individuals acting as Submission Specific Experts who are not from GSMA Members, Associate Members and Rapporteurs will sign and adhere to a personal NDA (available at Annexe Annex C).

The GSMA will not communicate details of the vulnerability outside of the SCG or GSMA Members, Associate Members and Rapporteurs without the agreement of the Reporter.

Annex A GSMA CVD History

Security vulnerabilities exist in most, if not all, software and hardware products and services. These are frequently exploited to cause service providers and their customers harm.

A disclosure framework such as a CVD programme, is a key component to encourage constructive and structured engagement with security researchers. Facilitating early remediation of vulnerabilities and responsible and controlled public release of the vulnerability details. Consequently, a CVD programme is an important component of improving security awareness and readiness for any organisation.

For several years the GSMA supported security researchers to disclose vulnerability details in a responsible manner on an informal basis, allowing remediation to take place prior to public disclosure. Based on the success of this informal service the GSMA developed a formal CVD process to manage industry impacting security issues.

In 2017, the GSMA's Fraud and Security Group (FASG) [10] defined and supported the creation of this unique industry focused programme. The service invites security researchers who have discovered vulnerabilities or weaknesses in mobile systems to disclose details to GSMA. In turn allowing GSMA member organisations, who are manufacturers and providers of products and services, to address the identified security issues before public disclosures enable exploitation.

The GSMA is able to convene industry subject matter experts to assess the research, often highly technical in nature, and offer remediating advice for short, medium and long term fixes, where appropriate. The GSMA is then able to share details of these fixes with the entire membership; with the intention to prevent exploitation.

The GSMA membership is also in a unique position to influence the industry standardisation process, allowing vulnerabilities to be designed out at the earliest phase of network design.

The benefit of such a Programme for the GSMA membership is the convening of industry experts to collectively address and prevent attacks capable of exploiting disclosed vulnerabilities. The benefit for the security researchers' is that they receive a constructive and structured engagement with the industry and can contribute to enhancing the security of mobile services.

Annex B CVD Document Templates

Reporters may supply information on the vulnerability by email using the Submission template below. GPG encryption is encouraged but not required, the public key can be found at [4]. Both form formats can be found on www.gsma.com/cvd

B.1 Email Format

Contact Details

Name (Full or Nickname Mandatory)

Organisation

Email Address (Mandatory)

Telephone

Can we provide your details to GSMA stakeholders (Yes/No)

Do you want to be acknowledged publicly (Yes/No)

Vulnerability Details (All below are mandatory)

Title of vulnerability

Description of vulnerability

Product or service name

Date vulnerability found

Is the vulnerability still live? (Yes/No)

Do you believe the vulnerability is currently being exploited? (Yes/No)

Probability of reproduction of vulnerability (Always / Often / Rarely)

Possible threat caused by the vulnerability

Can you provide PoC Code, Screenshots or other useful information?

Do you intend to let us review the vulnerability before going public? (Yes/No)

To what other organisation(s) has the vulnerability been disclosed?

B.2 Word Template

Reporter Details	
Name (either full or nickname): ***(Mandatory Field)***	
Organisation	
Email *(Mandatory Field)*	
Telephone	
Can we provide your details to another organisation or company if required for coordination	No ☐ Yes ☐
Do you want to be publicly acknowledged	No ☐ Yes ☐
Vulnerability Details ***(All below are mandatory fields)***	
Title of Vulnerability	
Description of Vulnerability	
Product or Service Name	
Date Vulnerability Found	
Is the Vulnerability still live	No ☐ Yes ☐
Do you believe the vulnerability is currently being exploited	No ☐ Yes ☐
Probability of reproduction of vulnerability	1 – Always ☐ 2 – Often ☐ 3 – Rarely ☐
Possible threat caused by the vulnerability	
Can you provide any PoC Code, Screenshots or Http requests etc.	
Do you intend to let us review the vulnerability before going public	No ☐ Yes ☐
To what other organisation(s) has the vulnerability been reported?	

B.3 CVD Close Down Template

Coordinated Vulnerability Disclosure - Close Down Information	
GSMA CVD Number	
CVD Title	
Reporter	
Organisation	
Has the CVD Submission been resolved?	No ☐ Yes ☐
Have the Reporters been informed of closure?	No ☐ Yes ☐
Have any concerned parties been informed?	No ☐ Yes ☐
Summary/Resolution of Vulnerability	
Date Vulnerability Found	
Date Vulnerability Closed	
Has the vulnerability been publicly disclosed?	No ☐ Yes ☐
Has this CVD Submission been entered into Mobile Security Research Hall of Fame?	No ☐ Yes ☐
Has a request for Reporter feedback been issued?	No ☐ Yes ☐
Any Further Notes	

B.4 Example Panel of Experts (PoE) Application Form

Applicant Details			
Name:			
Company: *(As listed on your GSMA IC2 account)*			
Work email:			
Telephone:			
I am a member of the GSMA Fraud and Security Group (FASG):		No ☐ Yes ☐	
Geographical areas of company activity: *(Tick all that apply)*	North America ☐ Latin/South/Central America ☐ Middle East & North Africa ☐ Sub-Saharan Africa ☐ Europe ☐ Russia/Central Asia ☐ Greater China ☐ India and South Asia ☐ East and South-East Asia ☐ Oceania ☐		
Applicant Experience			
Subject matter areas: *(Please select the area/s in which you have expertise.)* * Including design, planning, implementation, operation, incident handling		**Real World Experience***	**Standards /Governance**
	Transport/transmission security	☐	☐
	Radio access network security	☐	☐
	Signalling protocol security	☐	☐
	Core network technology security	☐	☐
	Device security	☐	☐
	UICC/eUICC security	☐	☐
	Cryptography	☐	☐
	Internet of Things (IoT) security	☐	☐
	Roaming and interworking security	☐	☐
	Cloud and virtualisation security	☐	☐
	Billing and financial system security	☐	☐
	Protocol analysis	☐	☐
	Other: _____		

Please outline any evidence of relevant experience within the areas above and with the wider mobile industry/academia *(e.g. standards, research, publications, and memberships of other committees/industry bodies):*

I have previously been a member of the GSMA CVD Panel of Experts (formerly Governance Team)?			No ☐ Yes ☐
Please provide referees who can be contacted by GSMA to support the application *(optional but recommended)*:	Referee One	Name:	
		Email:	
	Referee Two	Name:	
		Email:	
Applicant Consent			
I have read FS.23 and agree to be bound by the terms and conditions of the document set out therein:			No ☐ Yes ☐
I have received written approval by my employer to act as a member of the Panel of Experts:			No ☐ Yes ☐
Applicant Name:			
Signed:			
Date:			

Upon completion, please send to the GSMA CVD Director at cvd@gsma.com.

Any further information can be found at gsma.com/cvd.

Annex C Individual Non-Disclosure Agreement

MUTUAL NON-DISCLOSURE AGREEMENT

This Mutual Non-Disclosure Agreement (this **"Agreement"**) is entered into and effective as of **[INSERT DATE]** (the **"Effective Date"**) by and between

the **GSM Association** with an office at 2nd Floor, The Walbrook Building, 25 Walbrook, London EC4N 8AF, England and _____whose registered office is located at: _____(the "**Confidant"**) (each individually a "Party" and collectively the "Parties")

WHEREAS the Parties wish to protect the confidential nature of information disclosed under this Agreement.

NOW THEREFORE it is hereby agreed as follows:

1. DEFINITIONS

1.1 **"Affiliates"** means any subsidiary or holding company of an entity, any subsidiary of any of its holding companies and any partnership, company or undertaking (whether incorporated or unincorporated) in which an entity has the majority of the voting rights or economic interest.

1.2 **"Business Purpose"** means ***[INSERT PURPOSE FOR WHICH THE CONFIDENTIAL INFORMATION IS BEING EXCHANGED]***.

1.3 **"Confidential Information"** means all information of the GSMA Group, the Confidant or a third party, including without limitation, information relating to the research, development, business plans, marketing, operations, finances, personal data of any such entity, which is disclosed by one Party directly or indirectly to the other Party hereunder in connection with the Business Purpose, whether in writing (physically or electronically), visually or orally and which is designated as proprietary or confidential or which, under the circumstances, should reasonably be considered confidential.

1.4 "**Disclosing Party**" a Party to this Agreement that directly or indirectly discloses or makes available its Confidential Information to the other Party.

1.5 **"GSMA Group"** means the GSMA, its Affiliates and GSMA Members together with the directors, employees and agents of each of those.

1.6 **"GSMA Members"** means the full, associate and other members of the GSM Association.

1.7 "**Receiving Party**" means a Party to this Agreement which directly or indirectly receives or obtains the other Party's Confidential Information.

2. OWNERSHIP OF CONFIDENTIAL INFORMATION

All Confidential Information is, and shall remain, the property of the Disclosing Party. Nothing herein shall be construed as granting any rights by licence or otherwise in the Confidential Information except as expressly provided herein. Other than as expressly provided herein, no licence is granted (whether implicitly, by estoppel or otherwise) under any patents, copyrights, trademarks, database rights, semiconductor topography rights, registered or unregistered designs, utility models or other intellectual property rights relating to the Confidential Information.

3. OBLIGATIONS OF CONFIDENTIALITY

3.1 The Receiving Party may use the Confidential Information received hereunder solely for the Business Purpose.

3.2 For a period of three (3) years from the receipt of Confidential Information hereunder, the Receiving Party shall use the same degree of care and means that it uses to protect its own Confidential Information of a similar nature, but in any event not less than reasonable care and means, to prevent the unauthorized use or disclosure to third parties of such Confidential Information.

3.3 The Receiving Party shall disclose the Confidential Information only to its officers, employees, consultants, Affiliates, or contractors with a "need to know" for the Business Purpose and who have entered into confidentiality agreements sufficient to prohibit further unauthorized use or disclosure of the Confidential Information. The Receiving Party may not alter, decompile, disassemble, reverse engineer, or otherwise modify any Confidential Information received hereunder other than in furtherance of the Business Purpose and the mingling of the Confidential Information with information of the Receiving Party shall not affect the confidential nature or ownership of the same as stated hereunder.

3.4 This Agreement shall impose no obligation of confidentiality upon the Receiving Party with respect to any portion of Confidential Information received hereunder, which: (a) is already known in the public domain prior to this Agreement or becomes publicly known through no fault of the Receiving Party; (b) is or becomes known to the Receiving Party from a third party source other than the Disclosing Party without duties of confidentiality attached and without breach of any agreement between the Disclosing Party and such third party; (c) is furnished to another by the Disclosing Party without restriction on disclosure; or (d) was independently developed by the Receiving Party without the benefit of the Confidential Information.

3.5 Nothing in this Agreement shall prevent a Receiving Party from disclosing Confidential Information to the extent it is legally compelled to do so by any governmental investigative or judicial agency pursuant to proceedings over which such agency has jurisdiction; *provided, however*, that prior to any such disclosure, the Receiving Party shall: (a) assert the confidential nature of the Confidential Information to the agency; (b) immediately notify the Disclosing Party in writing of the agency's order or request to disclose; and (c) provide all reasonable cooperation to the Disclosing Party in protecting against any such disclosure and/or obtaining a protective order narrowing the scope of the compelled disclosure and protecting its confidentiality.

3.6 Each Party agrees that this Agreement applies equally to all Confidential Information concerning the Business Purpose shared by the Disclosing Party or any Affiliate of the Disclosing Party to the Receiving Party prior to the Effective Date.

4. EXCLUSIVE ACTIVITY

Nothing in this Agreement shall prevent a Party from pursuing similar discussions with third parties provided that there is no breach of the obligations of this Agreement. The obligations of confidentiality under this Agreement shall not be construed to limit a Party's right to develop independently or acquire products or services without use of the other Party's Confidential Information.

5. TERM AND TERMINATION

5.1 The term of this Agreement is for a period of one (1) year from the Effective Date unless otherwise terminated.

5.2 Either Party may terminate this Agreement for any reason prior to the period stated in clause 5.1 upon thirty (30) days' written notice to the other Party.

5.3 Either Party may terminate this Agreement immediately upon written notice to the other in the event of any breach by that other Party of this Agreement.

5.4 Upon the written request of either Party or upon the expiration or termination of this Agreement for any reason the Receiving Party will promptly return all copies of the Disclosing Party's Confidential Information in its possession, power, custody or control, or in respect of Confidential Information held electronically permanently erase to the extent technically feasible (without incurring excessive expense).

5.5 Notwithstanding anything else contained herein, each Party may retain a copy of the other Party's Confidential Information to the extent required for legal or regulatory purposes. Any Confidential Information that is retained under this clause or which has not been returned, destroyed or permanently erased under clause 5.4 shall remain subject to the other provisions of this Agreement.

5.6 Clauses 1, 2, 3, 4, 5.4, 5.5, 6 and 7 shall survive the expiration or termination of this Agreement.

6. NO WARRANTY; DISCLAIMER

NEITHER PARTY MAKES ANY REPRESENTATION, WARRANTY OR UNDERTAKING (EXPRESS OR IMPLIED) WITH RESPECT TO, AND DOES NOT ACCEPT ANY RESPONSIBILITY FOR, (AND HEREBY DISCLAIMS LIABILITY FOR), THE ACCURACY OR COMPLETENESS OF ANY CONFIDENTIAL INFORMATION. NEITHER PARTY IS RESPONSIBLE FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FINANCIAL OR OTHERWISE CASUED DIRECTLY OR INDIRECTLY BY RELIANCE UPON THE CONFIDENTIAL INFORMATION. NEITHER PARTY IS UNDER ANY OBLIGATION TO PROVIDE THE OTHER PARTY WITH CONFIDENTIAL INFORMATION AND MAY AT ANY TIME AND IN ITS SOLE DISCRETION DISCONTINUE ITS DISTRIBUTION. ALL CONFIDENTIAL INFORMATION IS PROVIDED "AS IS".

7. GENERAL

7.1 Equitable Remedies. The Parties agree that there is no adequate remedy in damages for any breach of the obligations of confidence hereunder and upon any such breach or any threat thereof by the Receiving Party, the Disclosing Party shall be entitled to seek appropriate equitable relief, including injunctive relief in addition to whatever other remedies it might be entitled, including, but not limited to, damages.

7.2 Severability. If any term, provision, covenant or condition of this Agreement is held invalid or unenforceable for any reason, the Parties agree that such invalidity shall not affect the validity of the remaining provisions of this Agreement and further agree to substitute for such invalid or unenforceable provision a valid and enforceable provision of similar intent and economic effect.

7.3 Publicity. Neither Party, without the other Party's prior written approval, shall make any public announcement or any disclosure as to the existence of or matters set forth in this Agreement.

7.4 Assignment. Neither Party may assign its rights or obligations under this Agreement.

7.5 Waiver. The failure of a Party at any time to require performance by the other Party of any provision hereof shall not affect in any way the full right to require such performance at any time thereafter. Nor shall the waiver by a Party of a breach of any provision hereof be taken or held to be a waiver of the provision itself.

7.6 Headings. The headings in this Agreement are provided for convenience only and do not affect its meaning.

7.7 Relationship of the Parties. Nothing in this Agreement will be construed as creating an employer-employee or agency relationship, a partnership or a joint venture between the Parties.

7.8 Governing Law.

[This Agreement shall be construed in accordance with, and all disputes hereunder shall be governed by, the laws of England and shall be subject to the exclusive jurisdiction of the English courts.]

7.9 Facsimiles; Email. The Parties agree to treat documents sent via telephonic facsimile or email as original documents, *provided that* either Party may require the other to provide a manually executed or authenticated original or duplicate of any document so sent within a reasonable period of time, and if such original or duplicate is not provided within that time, then to treat the document as not having been received initially until the manually executed or authenticated original or duplicate is delivered.

7.10 Entire Agreement; Modification. This Agreement is the complete, final and exclusive statement of the terms of the agreement between the Parties and supersedes any and all other prior and contemporaneous negotiations and agreements, whether oral or written, between them relating to the subject matter hereof. This Agreement may not be varied, modified, altered, or amended except in writing signed by the Parties.

7.11 Counterparts. This Agreement may be executed in two (2) or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF the Parties have caused this Agreement to be executed by their duly authorized representatives on the date(s) shown below.

GSMA	**NAME OF OTHER COMPANY**
_____	_____
Signature	Signature
_____	_____
Printed	Printed
_____	_____
Title	Title
_____	_____
Date	Date

Annex D Document Management

D.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	13/3/2017	First published version	PSMC	Ethan Duffell, GSMA
2.0	29/5/2019	Addition of closedown template and changes to governance team structure. Minor editorial changes.	TG	Samantha Kight, GSMA
3.0	15/7/2020	Formalising GSMA CVD policy, member application process, roles and responsibilities, unifying document language, remove GSMA own assets (e.g. website) from scope.	FASG	James Skuse, GSMA

D.2 Other Information

Type	Description
Document Owner	GSMA Fraud and Security Architecture Group (FSAG)
Editor / Company	James Skuse, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.