## Contents

1. Chairman’s Statement ........................................... 4
3. Outlook for FY 2019-2020 .................................... 9
4. Corporate Governance and Leadership ...................... 13
5. Committees ....................................................... 17
6. Advisory Groups ................................................ 20
7. Membership Types and Observer Status .................... 22
8. Membership and Observer Benefits .......................... 25
9. Our Services ....................................................... 28
10. Our Intellectual Property Rights Model ...................... 31
11. Financial Position ............................................... 37
Chairman’s Statement
Chairman’s Statement

Dear Stakeholders,

Since the founding of Secure Chorus, as a not for profit membership organisation, our vision has been consistent: to become a thought leader in the development of multi-brand ecosystems of cybersecurity products and services that adopt the Secure Chorus technical approach of “interoperability, security and auditability by design.”

The world is facing a growing number of complex and interconnected cybersecurity challenges. In isolation, these are daunting. Faced simultaneously, we will struggle if we do not work together. There has never been a more pressing need for a collaborative and multi-stakeholder approach to shared global cybersecurity problems.

Our mission is to serve as a platform for multi-stakeholder co-operation for the development and adoption of common technology standards by multi-brand ecosystems of technology products that have a requirement for interoperability, security and auditability by design.

FY 2018-2019 was another strong year of strategic execution for Secure Chorus, marked by the establishment of important governance structures, including the Strategy Committee and the Standards Committee, as well as thought-leadership structures including the inward-focusing Standardisation Track Technical Activity, the Implementation Track Technical Activity and the outward-focusing Thought Leadership Platform initiative.

We are very proud to announce that in this past financial year we developed a technology roadmap that meets our members’ and market requirements. We published our first set of interoperability standards for encrypted voice calls specifically aimed at enterprise users and which has created a much-needed breakthrough, setting a strong step ahead to develop interoperability standards for developers of multimedia apps.

Our public engagement strategy was aimed at providing an in-depth yet accessible flow of content, offering insight into topics and challenges that occupy the attention of private and public sector leaders. Secure Chorus writing credits on the topic of cybersecurity include articles published in influential British and international media. Secure Chorus also established new strong relations with important information security, standards and industry forums, as well as continuing to foster established ones. The results of this strategic focus originated several invitations to speak at important global forums.

Over the past year our membership base has continued grow, while our existing members have renewed their engagement, reflecting their commitment to – and expectations from – Secure Chorus as a global platform for multi-stakeholder cooperation and impact. Our members are world-class organisations, including governments, public sector, private sector and academia with a strong interest in developing capabilities for solving key information security challenges. They are the driving force behind Secure Chorus’ programmes.

It is satisfying that many of our achievements continue to be the direct outcome of the collaborative efforts between the public and private sector to establish Secure Chorus as a global community of thought leaders that believe passionately in the power of multi-stakeholder engagement and open standards to address the secure communication challenges of our global digital economy.

We are also extremely proud to report that Secure Chorus has played a key role in supporting the UK National Cyber Security Centre’s work to make “the UK the safest place to live and do work on line.” The importance of our work was underlined by the fact that the UK Government renewed its commitment to fund Secure Chorus as part of its £1.9bn transformation investment in the UK’s National Cyber Security Strategy.

I would like to thank everyone for making FY 2018-2019 a successful year. We look forward to another year of providing the necessary common standards and capabilities for making our global digital environments safer.

Elisabetta Zaccaria
Chairman
2 Annual Report FY 2018-2019
Secure Chorus FY 1 April 2018 – 31 March 2019 was marked by strong achievements. We worked to deliver against our ambitious vision to serve as a platform for multi-stakeholder cooperation in the field of information security to develop forward-looking strategies, common standards and tangible capabilities for a safer global digital economy.

Efforts this year were focused on strategic priorities including the development and implementation of new thought leadership and governance structures to enable our members to engage in collaborative initiatives.

Focus was also placed on public engagement initiatives to promote acceptance of Secure Chorus’ technical approach – “interoperability, security and auditability by design” – through open contributions with the wider public, as well as demonstrations and engagement with technical forums.

Secure Chorus’ members continuous engagement has been critical to our achievements in the past financial year. We are pleased to report that during this period, the number of new members increased by 45 percent, while 90 percent of existing members renewed their engagement, reflecting the international business community’s commitment to, and expectations from, Secure Chorus as a global platform of public-private sector interaction, insight and impact.

Two important governance structures have been established to accelerate and amplify our members’ engagement to provide advice to our Board of Directors. This past fiscal year saw the launch of the Strategy Committee and the Standards Committee.

Following the establishment of our Standards Committee in April 2018, successful advisory work began to support the Board of Directors in the development of a technology roadmap that meets our members’ and the market requirements. The Strategy Committee also played a key role in advising the board on standards and test plans prior to being published.

The Strategy Committee was established in December 2018 and provides a strong sounding board that has shaped our corporate strategy for FY 2019-2020.

We implemented a key outward-focused thought leadership initiative – the “Thought Leadership Platform” – to intensify our effort to establish Secure Chorus and its members’ community as a forum that shapes agendas for public-private cooperation in the context of a rapidly-evolving global digital environment characterised by information security challenges that require knowledge sharing and building across sectors.

Following the establishment of our Thought Leadership Platform pilot, work began in FY 2018-2019 on developing and running a series of successful Thought Leadership Platforms throughout the past fiscal year for the financial services, healthcare and sport sectors. These included the following hosts: the National Health Service (NHS), the Football Association (FA) and the Institute of Chartered Accountants in England and Wales (ICAEW).

Focus was placed on setting up two thought leadership forums focused on our technology work: the “Standardisation Technical Track Activity” and the “Implementation Technical Track Activity” to co-design with our members the relevant interoperability standards-related test plans and to then pilot their adoption into our members’ technologies.
These structures were proven to be key to our ability in leveraging the depth and breadth of Secure Chorus’ members’ technical knowledge, thus empowering our members to shape our technology strategy while ensuring Secure Chorus publishes best-of-breed standards.

Following the establishment of our Standardisation Technical Track Activity, work began on implementing our technology roadmap that included the publication of our first set of interoperability standards for encrypted voice calls specifically aimed at enterprise users and which has created a much-needed breakthrough, setting a strong step ahead to develop interoperability standards for developers of multimedia apps.

In the past financial year, we saw numerous achievements across our public relations activities.

The beginning of FY 2018-2019 was marked by an important press release issued in April 2018 by the UK Government, in which Secure Chorus was acknowledged as the “public-private collaboration forum for long-term security of the global digitally enabled economy.” This was part of the National Cyber Security Centre announcement that it had formally joined Secure Chorus as its first Government Member.

Secure Chorus published 2 white papers and 17 articles on relevant information security topics, including identity-based public key cryptography, quantum computing and post-quantum cryptography, data security, interoperability standards in information security, secure mission-critical communication and compliance with data security and the EU GDPR, as well the EU PSD2. Secure Chorus authored articles and contributed comments to publications specialising in different sectors, including information security, emergency services, critical national infrastructure (CNI), internet of things (IOT), financial services, legal and healthcare.


Secure Chorus also forged strong new relationships with important information security, standards and industry forums, while continuing to foster established ones. The results of this strategic focus originated several invitations to speak at important forums including: CYBERUK 2018, British Private Equity and Venture Capital Association (BVCA), London Society of Chartered Accountants (LSCA) and The European Telecommunications Standards Institute (ETSI).
Outlook for FY 2019-2020
Outlook for FY 2019-2020

The Information and Communications Technology (ICT) industries are at the heart of the ongoing global digital transformation. Rapid advances in computing and connectivity technologies are creating simultaneously immense opportunities for development and extraordinary information security challenges for both the private and public sectors.

Secure Chorus’ vision for FY 1 April 2019 – 31 March 2020 is to be become a thought leader in the development of multi-brand ecosystems of cybersecurity products and services that adopt the Secure Chorus technical approach: “interoperability, security and auditability by design.”

Our work in the new financial year will focus on achieving our mission to serve as a platform for multi-stakeholder co-operation for the development and adoption of common technology standards by multi-brand ecosystems of technology products that have a requirement for interoperability, security and auditability by design.

In alignment with our vision and mission we set ourselves two high level objectives for FY 2019-2020:

• To support the development and implementation of common technology standards, where such standards are to be adopted by multi-brand ecosystems of technology products that have a requirement for interoperability, security and auditability by design.

• To promote acceptance of Secure Chorus’s technical approach, through open contributions to the wider public, as well as demonstrations and engagement with important technical forums.

Together with our members’ community, we will spearhead multiple initiatives to achieve our objectives, including:

BUILDING CAPABILITIES FOR THE ICT SECURITY INDUSTRY

• Building common interoperability standards for the future of multi-media applications

In FY 2019-2020 we will work with Secure Chorus’ members, which are application developers and ICT security specialists, to deliver against an ambitious technology roadmap of interoperability standards that, once implemented by our members, will give genesis to a multi-brand ecosystem of multi-media applications which are all “interoperable, auditable and secure by design”. This will be achieved through adoption into their products by different member organisations of MIKEY-SAKKE open cryptography standards and Secure Chorus interoperability standards.

In order to ensure our members have effectively adopted Secure Chorus’ interoperability standards we will focus on developing and implementing our first “Self-Certification Scheme”. The Scheme will enable our members who are application developers to use a set of Secure Chorus’ test-plans to self-certify that their applications comply with one or more Secure Chorus’ interoperability standards as published from time to time.
• Exploring common interoperability standards to connect Mission-Critical Push-To-Talk (MCPTT) with multi-media application

In the previous financial year, we published a white paper as well as several articles on emergency services that explored the topic of developing bespoke interoperability standards to connect Mission-Critical Push-To-Talk with Secure Chorus members’ multi-media applications.

The 3rd Generation Partnership Project (3GPP) has defined the “Security of Mission-Critical Service”, mandating the open cryptography standard MIKEY-SAKKE to be used for encrypting data and providing cryptographic keys.

While the standards developed by 3GPP ensure interoperability between users of MCPTT systems, in certain scenarios emergency services organisations may also need to communicate securely with other stakeholders that may not be users of typical emergency services equipment on a day-to-day basis.

One of the solutions for users not using MCPTT on a day-to-day basis is to adopt multi-media applications developed by some of Secure Chorus’ members. These are communication applications that provide the benefits of MIKEY-SAKKE and its unique key management approach. Because some Secure Chorus members are already integrating MIKEY-SAKKE into their applications and products, there is now a much lower bar to developing interoperability standards to connect MCPTT with these communication apps.

In FY 2019-2020 we will work with Secure Chorus’ members which are application developers and ICT security specialists to explore the challenges that need to be resolved to develop interoperability standards to connect Mission-Critical Push-To-Talk with Secure Chorus members’ multi-media applications.

• Exploring quantum-resistant cryptographic solutions

In the previous financial year, we published a white paper on quantum-resistant cryptography solutions, as well as several articles. We also ran internal and external Thought Leadership Platforms to provide education on the subject to Secure Chorus’ members, as well as to the financial services industry.

In FY 2019-2020 we will continue to work with Secure Chorus’ members from government, industry and academia which are specialist in quantum-resistant cryptographic solutions to explore the replacement of MIKEY-SAKKE with a quantum-safe alternative, taking into consideration the implications for protocol designers. We will focus on lattice-based cryptography, which is one of the most promising areas in quantum-resistant cryptography.

BUILDING KNOWLEDGE OF ICT SECURITY ACROSS OUR SECTORS OF FOCUS

In the previous financial year, Secure Chorus worked closely with its government and industry members with a shared view that cybersecurity is a common interest and responsibility. Our intention was to deepen the spirit of co-operation beyond our membership base and engaged with several industries, which we believed would benefit from learning about our approach to ICT security, based on common technology standards, which if adopted into two or more ICT products would create an ecosystem of products that are interoperable, secure and auditable by design.
In FY 2019-2020, our public relations strategy will focus on offering our members’ community and senior executives across sectors an unrivalled platform for ICT security debate and knowledge building, which we see as the home of common technology standards and capabilities.

We will achieve this by focusing on two main activities: first, by building world-class relationships and maintaining continuous contact with the most relevant media worldwide; and second, by developing initiatives that reach audiences across our sectors of focus, namely financial services, legal services, healthcare and the internet of things (IOT).

Our aim is to position Secure Chorus as a thought leader in secure communications, as the home of common technology standards and best practices for the ICT security industry, as well as serving as a marketplace for procuring technology solutions for governments and enterprise, providing solutions that are interoperable, secure and auditable by design.
Corporate Governance and Leadership
4 Corporate Governance and Leadership

Corporate Governance

Incorporated as a company limited by guarantee in 2016 and headquartered in London, UK, Secure Chorus Ltd is a not-for-profit membership organisation.

During its Launch Period, Secure Chorus Ltd has a special governance structure, as outlined in the Articles of Association (hereinafter “Statue”). The Launch Period is the period during which Secure Chorus Ltd is funded by the National Cyber Security Centre, as part of the UK Government’s £1.9bn transformation investment in the UK’s National Cyber Security Strategy.

Board of Directors

The main governing body of Secure Chorus Ltd is its Board of Directors: it determines and supervises the activities of Secure Chorus Ltd and its governing bodies, including approving the annual accounts and strategic direction, as well as managing its statute.

The Chairman

The Chairman presides over the board of directors. The Chairman is responsible for Secure Chorus Ltd strategy and represents the organisation to the relevant internal and external stakeholders.

The Chairman works in close collaboration with the Board of Directors and the company’s management, ensuring that Secure Chorus Ltd strategy, institutional development and governance are aligned.
Leadership

Elisabetta Zaccaria, Chairman of the board

Ms Zaccaria is the Chairman of the Board of Directors and has oversight of the strategic direction of Secure Chorus Ltd. She is a thought leader, with more than 15 years’ of cybersecurity industry experience in several influential C-level positions. Ms Zaccaria co-founded Secure Chorus Ltd in 2016. Prior to this appointment, she was Group CSO and COO of Global Strategies Group, where she played a key leadership role as chief strategist between 2006 and 2012, turning the British start-up into a US$600 million-revenue international business in six years. She has also held non-executive director roles in several companies in the UK, US, Luxembourg and the Netherlands.

In 2009, she was part of the top leadership team that was awarded the ‘ACG National Capital Deal for the Year Award, under US$100m’. During the most challenging economic climate in decades, her team successfully completed the first USA government services sector IPO on Nasdaq of a technology company in three years, with a deal valued at US$63 million. In 2019, she was featured in the book ‘Women Know Cyber: 100 Fascinating Females Fighting Cybercrime’, published by Cyber Security Ventures, spotlighting leading female professionals who stand out for their contributions in fighting global digital crime. In 2018, she was also mentioned by Cybercrime Magazine as one of the “132 Women in Cybersecurity to Follow on Twitter.”

Her academic qualifications include a Master of Jurisprudence from University of Ferrara (Italy) and a Master of Arts in International Relations and Affairs from Hult International School of Business (United Kingdom). She is an alumnus of the London Business School, having attended executive education in corporate finance.

Stephen Brown, Director of the board and Chief Information Officer

Mr Brown serves as director of the board and has oversight of technology aspects of Secure Chorus including technical management, setting the technical strategy and representing the technology externally as of 1 April 2019. Prior to that, he managed all IT and technology aspects of Secure Chorus. Mr Brown has more than 25 years’ experience in providing technology solutions, including technical architecture, cybersecurity, design, system development and management of information systems. He served as Head of IT for various organisations across sectors, including defence and national security, technology, oil and gas, commodity extraction processes, manufacturing and professional services industries. He is professionally qualified in programme and project techniques such as MSP (Managing Successful Programmes), Prince2 and Agile Project Management.

Roderick Hodgson, Director of the board

Mr Hodgson served as director of the board and had oversight of the technology aspects of Secure Chorus, including technical management, setting the technical strategy and representing the technology externally. Mr Hodgson stepped down on from the post on 31 March 2019.
Ruth Davis, Chief of Staff

Mrs Davis has oversight of the operational aspects of Secure Chorus. She has more than 15 years’ of experience in management, operations, project management (PRINCE2 Practitioner qualified), knowledge exchange, entrepreneurship and SMEs, as well as marketing and communications. She has held several senior management roles at UCL Innovation and Enterprise (formerly UCL Advances), supporting the full lifecycle of technology start-ups and SMEs in London. Mrs Davis holds a Master of Business Administration (MBA) from Kingston University.

Robert Mears, Financial Controller

Mr Mears has oversight of all financial aspects of Secure Chorus. He has more than a decade of senior leadership experience as Finance Director and Managing Director for a number of companies across the cybersecurity, technology, fashion and retail sectors. Mr Mears qualified as Chartered Accountant ACA at ICAEW and holds a BSc (Hons) in Civil Engineering from City University London.
Committees
5 Committees

Standards Committee

The Standards Committee was set up in April 2018. It is one of the five Membership Committees established by the Statute to advise the board on the interoperability standards, which establish the engineering and technical criteria pursuant to which different information technology systems and software applications may communicate, exchange data, and use the information that has been exchanged.

The Chairman, Chief Executive Officer, Chief Financial Officer, Chief Technology Officer of Secure Chorus Ltd and (as appointed from time to time) Government Members and Partner Members shall be entitled to be a member of the Standards Committee.

The Standard Committee shall be advisory in nature throughout the Launch Period and accordingly have no right to nominate an individual to the Board of Directors of Secure Chorus Ltd. Following the Launch Period, the Standards Committee shall have the right to nominate an individual to the board in accordance with the Statute.

Chair of Standards Committee:
Dr Andy Lilly

Vice-Chair of Standards Committee:
Dr Kit Kilgour

Members of Standards Committee:
Elisabetta Zaccaria, Chairman of the board, Secure Chorus
The National Cyber Security Centre
Dr Andy Lilly, Armour Communications
Adam Knight, Telefonica
Andrew Roberts, BAE Systems Applied Intelligence
Micael Berg, Cryptify
Mike Brown, ISARA Corporation
Dr Kit Kilgour, Sepura
Gerald McQuaid, Vodafone
Simon Pryce, Leonardo
Dr Nithin Thomas, SQR Systems
Sebastian Wiles, Serbus
Stuart McKean, Nine23
David Harker, Harker Labs
Governments Committee

The Government Committee is the Membership Committee consisting of Government Members which are either a supranational organisation or national government.

Corporates Committee

The Corporates Committee is the Membership Committee consisting of Partner Members which are body corporates with a turnover of more than £50 million per financial year.

SMEs Committee

The SMEs Committee is the Membership Committee consisting of Partner Members which are body corporates with a turnover of less than £50 million but more than £2 million per financial year.

MEs Committee

The MEs Committee is the Membership Committee consisting of Partner Members which are body corporates with a turnover of less than £2 million per financial year.

The Governments Committee, Corporates Committee, SMEs Committee and MEs Committee were not set up in FY 2018-2019.

Strategy Committee

The Strategy Committee was set up in December 2018. The Strategy Committee is not established by the Statute and therefore it was established with a resolution of the Board of Directors to advise the board on strategic initiatives.

The Strategy Committee was dissolved by resolution of the board of directors in July 2019, as part of a restructuring process that included new governance structures for members’ engagement on strategy.
Advisory Groups
6 Advisory Groups

Regulatory Compliance Advisory Group

Secure Chorus Ltd has one Advisory Group which has been established by Statue that provides recommendations, guidance and advice to the board of directors on regulatory compliance matters: the Regulatory Compliance Advisory Group.

The Regulatory Compliance Advisory Group was not set up in FY 2018-2019.
Membership Types and Observer Status
7 Membership Types and Observer Status

Secure Chorus’ Statute establishes the following classes of membership:

1. Launch Member
2. Government Member
3. Partner Member
4. Associate Member
5. Observer Status

Launch Member

Membership Criteria

Launch Member status in FY 2018-2019 was limited to two companies incorporated under the Company’s Act 2006: Cyber Y Ltd and Roderick Hodgson Ltd.

Government Member

Membership Criteria

Any supranational organisation or national government able to:
   I. have a 500 or more user-base utilising a Secure Chorus Compliant Product, service or infrastructure; or
   II. provide assistance in the establishment and development an ecosystem to support Secure Chorus Compliant Products, enabling them to be sustainable and trusted by the market. Such assistance may include:
      a. advice on the technical content of the Standards; and
      b. Standards authorship and development;

Partner Member

Membership Criteria

Any company incorporated under the Companies Acts, or any other body corporate that at the time of its application is:
   I. offering Secure Chorus Compliant Products, services and/or infrastructure; or
   II. developing, manufacturing or selling Secure Chorus Compliant Products; or
   III. having a 500 or more user base utilising a Secure Chorus Compliant Product, service or infrastructure; or
   IV. providing assistance in the establishment and development an eco-system to support Secure Chorus Compliant Products enabling them to be sustainable and trusted by the market, such assistance may include:
      a. advice on the technical content of the Standards;
      b. standards authorship and development;
      c. client and gateway review services, including accreditation; or
      d. interoperability testing and measurement.
**Associate Member**

**Membership Criteria**

Any company incorporated under the Companies Acts, or any other body corporate that meets the following criteria:

I. committed to developing Secure Chorus Compliant Products, services and/or infrastructure within an Agreed Period; or

II. committed to developing, manufacturing or selling products related to Secure Chorus Compliant Products within an Agreed Period;

III. or committed to developing a 500 or more user base of a Secure Chorus Compliant Products, service or infrastructure within an Agreed Period;

**Observer Status**

**Observer Criteria**

Any regulator, academic institution, standards organisation or trade association that is committed to assisting and/or promoting the Company within a period of 12 months.
8 Membership and Observer Benefits
8 Membership and Observer Benefits

Government Member Benefits

- Organisation’s name included in the Secure Chorus Register of Members
- Right to attend and vote at General Meetings of Members
- Right to vote on Ordinary and Special Resolutions of Members
- Eligibility to join Secure Chorus’ Governments Committee, Standards Committee and the Regulatory Compliance Advisory Group
- Right to vote on appointment of chairperson of Secure Chorus’ Governments Committee and Standards Committee
- Right to take part to the Standardisation Track Technical Activity and the Implementation Track Technical Activity
- Right to be part of the Secure Chorus’ Thought Leadership Platform
- Member’s logo highlighted on Secure Chorus’ website

Partner Member Benefits

- Organisation’s name included in Secure Chorus’ Register of Members
- Right to attend and vote at General Meetings of Members
- Right to vote on Ordinary and Special Resolutions of Members
- Eligibility to join Secure Chorus’ Standards Committee and Regulatory Compliance Advisory Group
- Eligibility to join either the Secure Chorus’ Corporate, SME or ME Committee depending on the Partner Member’s annual revenue
- Right to vote on appointment of chairperson of Secure Chorus’ Standards Committees
- Right to vote on the appointment of chairperson of either the Secure Chorus’ Corporate, SME or ME Committee depending on the Partner Member’s annual revenue
- Right to take part to the Standardisation Track Technical Activity and the Implementation Track Technical Activity
- Right to be part of the Secure Chorus’ Thought Leadership Platform
- Member’s logo and services or products highlighted on Secure Chorus’ website

Associate Member Benefits

- Organisation’s name included in Secure Chorus’ Register of Members
- Right to attend the General Meetings of Members
- Eligibility to join Secure Chorus’ Regulatory Compliance Advisory Group
- Eligibility to join either the Secure Chorus’ Corporate, SME or ME Committee depending on the Partner Member’s annual revenue
- Right to vote on the appointment of chairperson of either the Secure Chorus’ Corporate, SME or ME Committee depending on the Partner Member’s annual revenue
- Right to take part to the Implementation Track Technical Activity
- Right to be part of the Secure Chorus’ Thought Leadership Platform
- Member’s logo and services or products highlighted on Secure Chorus’ website
Observer Benefits

The Board of Directors may invite Observers to attend any Secure Chorus activity, including Membership Committee meetings, Thought Leadership Platforms and Standardisation Track Technical Activity and Implementation Track Technical Activity.
Our Services
Our Services

Our services focus on assisting organisations that embrace our technical approach, which is to develop standards to ensure technologies are interoperable, secure and auditable by design. These organisations may be from the ICT security or other technology sectors, which develop technology products that are IT-enabled and therefore require an information security strategy at the core of their products.

Our approach to these two ecosystems differs in some respects, inasmuch as organisations developing ICT security products and services are already expert in the field in which we operate, while the other type of organisations may only have a limited understanding of the information security aspects required.

The organisations in each ecosystem may simply decide to adopt the relevant standards into their products, or they may partner with one or more organisation as applicable in the same ecosystem, or from other ecosystems to gain a specific capability.

When an emerging or mature ecosystem approaches Secure Chorus to adopt our technical approach, we provide services to ensure it is easy for them to adopt MIKEY-SAKKE into their products (where applicable), and to ensure they are able to achieve interoperability between their products.

These services ensure the ecosystem is able to grow and prosper, and that it is able to ultimately serve the requirements of the one or more customer market it targets.

The provision of these services follows a process that can be broken down into different steps:

1. **Assessment of their technology strategy**

   Secure Chorus Ltd will first engage with the key participants in the ecosystem over the course of several meetings, in order to reach an understanding their technology strategy.

   **Assessment of their cybersecurity requirements**

   Secure Chorus Ltd will then perform an analysis of what the interoperability and security requirements of the ecosystem are, including the level of security required by the regulatory environment they operate in, and what auditability requirements may exist.

   **Assessment of their technologies to gauge technical approach**

   Together with the interoperability and security requirements of the ecosystem, Secure Chorus Ltd will then examine the technology products developed or used by the ecosystem, including assessment of their existing security standards in use by the participants in the ecosystem.

   If we are working with an ecosystem of information security products, we will assess if MIKEY-SAKKE is a suitable cryptography standard. For ecosystems of other technology products, we will investigate whether MIKEY-SAKKE can be integrated in their products to provide a higher grade of security.
2. Explaining the benefits of our technical approach to their ecosystem

If a suitable match has been found in the assessment of an ecosystem of technology products, Secure Chorus Ltd will then perform an outreach effort to present to the ecosystem the benefits of MIKEY-SAKKE and our technical approach. This will include hosting conversations with the organisations that have products forming part of ecosystem, together with existing stakeholders of Secure Chorus Ltd, such as the National Information Security Centre (a globally recognised centre of excellence in the field of information security), other government agencies with expertise in this field, and industry leaders in information security and post-quantum cryptography.

Through this activity, organisations forming part of the ecosystem will have the opportunity to share industry knowledge and to collaborate with veteran members of Secure Chorus Ltd that are part of ecosystems providing information security products.

3. Development of a bespoke technology roadmap

Secure Chorus Ltd will work with the organisations that have products forming part of an ecosystem to open a new stream of work and set a bespoke technology roadmap for the development of interoperability standards. This includes the hosting of technical meetings for the development of new standards and the authoring of new standards ("Standardisation Track Technical Activities"), as well as the hosting of technical meetings for fostering adoption of the standards and the authoring of new documents to facilitate the testing of interoperability ("Implementation Track Technical Activities").

Members will then have access to the standards and other relevant documents, all under a clear and coherent IPR framework.
Our Intellectual Property Rights Model
10 Our Intellectual Property Rights Model

The Company has a mandatory intellectual property rights policy that is set out in the Membership Application Form of the Company, and therefore applies to the Company and all of its members/observers.

Introduction

The objects for which the Company is established are the development and publishing of MIKEY-SAKKE protocol-based interoperability standards. In the pursuance of its activities, the Company may refer to, or make use of, patents and IP protected by IPR legislation. Diligent conduct in respect of these rights is essential to the Company’s functioning, good reputation, authority, sustainability and the achievement of its core objectives.

Scope

The aim of the IPR policy is to ensure the Company and its members/observers are aware of their responsibilities and obligations in relation to IPR, in order to minimise risk of infringement of patents and IP, and to ensure members/observers are committed to fair licencing terms of any patents related to the standards (field patents).

The Company IPR Policy applies to all activities undertaken by the Company and its members/observers, regarding the development, convergence and adoption of MIKEY-SAKKE-based interoperability standards for the secure communications industry.

Summary of the IPR Policy

Declaration of Field Patents

“Field Patents” means any Patent(s) owned by a member/observer, or an Affiliate of a member or observer, which would be infringed by the manufacture, sale, supply, lease, repair, use, importation, keeping, or otherwise disposal of any product that operates in accordance with any optional or mandatory part of a Standard such that it is not possible on technical (but not commercial) grounds to operate in accordance with any Standard without infringing that Patent. In the event that the technical solution prescribed in the Standard infringes different Patents depending upon how that Standard is implemented all such patents shall be considered to be Field Patents.

On becoming a member/observer, each shall provide the Company with a written declaration identifying its patents that are or may reasonably become Field Patents.

Thereafter, each member/observer shall use reasonable endeavours to provide the Company with a declaration identifying when a standard or any other deliverable may require the use of any Field Patent owned by that member/observer. Such declaration must be provided in a timely manner, and in particular
if a member or observer is submitting a proposal for a Deliverable (including a Standard), such proposal should identify Field Patents, or potential Field Patents, for which a Declaration must be provided within 48 hours of submission.

The above obligations do not require that members/observers carry out searches for any Field Patents.

Members/observers are also not compelled to contribute any specific patents to any deliverable, but should they choose to do so, and should the relevant patents become Field Patents, then there is an obligation to make a declaration, which must be submitted to the Company within 14 days of such Patents becoming Field Patents, or within 14 days of that Member or Observer identifying a Patent as a potential Field Patent, whichever is the sooner.

If a member/observer fails to make a declaration, they will be deemed to have provided the undertaking relating to the Field Patents that should have been the subject of such Declaration, as defined below.

**Licensing of Field Patents**

Where a member/observer becomes aware that it owns a patent that is, or may become, a Field Patent it must provide an irrevocable undertaking on the relevant declaration form that they are prepared to grant a non-exclusive licence of all of their field patents to manufacture (and have manufactured), sell, offer for sale, import, use or keep any product or service or method which operates in accordance with, or conforms to the Standard only in so far as it is necessary for the product, service or method to comply with the Standard:

- on FRAND Terms; and
- to any person or entity wishing to make use of the deliverable(s).

Such undertaking must bind all successors in title and affiliates, save where specific affiliates are noted on the Declaration as not being bound by the Undertaking.

Any Undertaking that a member or observer provides can be made conditional upon a reciprocal Undertaking from any prospective licensee in respect of their Field Patents.

The member/observer may refuse to provide an Undertaking to licence only if the patents are:

- not based on any Activity;
- developed independently of any other member/observer;
- not developed with the intention to be part of a deliverable; and
- declared on a Declaration form.

If any member/observer refuses to provide an Undertaking, or if the Company does not accept (acting reasonably) the reasons that the member/observer has provided in the Declaration form for refusing to provide the Undertaking, then that member/observer will lose their rights to participate in the relevant activity and develop any deliverable arising from it.

If, prior to the publication of a deliverable (including a standard) a member/observer refuses to give
the Undertaking in respect of certain Field Patents, then the Company shall review the deliverable and identify alternative technology that does not infringe that patent. The above loss of rights to participate will continue to apply if alternative technology is identified unless the Company, at its sole discretion, determines otherwise.

If any Field Patent is not identified prior to the publication of a deliverable, the member/observer that owns the Field Patent undertakes to provide a Declaration that includes an Undertaking in respect of that patent within 14 days of the member or observer recognising that they have a Field Patent.

If a Third-Party Field Patent is identified prior to the publication of a deliverable, the member/observer that identified the Third-Party Field Patent will ask the Third-Party owner if it is prepared to give an undertaking. If the Third-Party refuses to do so, then the Company shall review the deliverable and identify alternative technology that does not infringe that Third-Party Field Patent.

If the Third-Party Field Patent is identified after the publication of a deliverable the member or observer that identified the Third-Party Field Patent will ask the Third-Party owner if it is prepared to give an Undertaking. If the Third-Party refuses to do so, then the Company shall withdraw the Deliverable (including revoking the Standard) and review the Deliverable to identify alternative technology that does not infringe that Third-Party Field Patent. If no alternative technology is identified, the Deliverable shall remain withdrawn until such time as either an Undertaking is provided in respect of the Third-Party Field Patent, or alternative technology is identified.

The Company shall form an advisory group prior to 31 March 2021 to attempt to agree a policy and/or guideline as to what FRAND Terms are for a licence under any Field Patent (the “FRAND Guidelines”). Should the committee reach agreement as to appropriate FRAND Guidelines, the FRAND Guidelines shall be presented to the members at an extraordinary general meeting for approval by a special resolution.

**Deliverables**

All copyright, other than any original contribution Intellectual Property that is contributed by a member or observer, in any Deliverable shall be owned by the Company.

The Company shall make copies of all issued Deliverables available to members free of charge.

If Deliverables are marked by the Company (at its sole discretion) as “members only”:

- Members may make copies of the Deliverables for their own use, but may not distribute copies to third parties, or communicate their content to anyone who is not a member without the Company’s prior written approval; and
- Observers may not be provided with a copy of the Deliverable without the Company’s prior written approval.
- If an observer is provided with a copy of the Deliverable the observer may make copies of the Deliverables for its own use, but may not distribute copies to third parties, or communicate their content to anyone who is not a member without the Company’s prior written approval.
- If Deliverables are not marked by the Company (at its sole discretion) as “members only”, members or the Company may make copies of the Deliverables available to the public free of charge.
Intellectual Property and Field IP

All trademarks owned by the Company can be used by members/observers only while they remain members/observers and on the basis that such use is in accordance with the Company’s brand guidelines which are located on the Company’s website at www.securechorus.org as may be updated from time to time. Any goodwill that accrues as a result of such use shall accrue automatically and exclusively to the Company. Members/observers shall not make any statements on behalf of the Company without the Company’s prior written approval.

It is the member/observer's responsibility to determine whether any IP that is contributed to an activity requires the prior consent of another party to be used by the Company and other members/observers, and if so, to obtain that consent.

By contributing IP to an activity, the member/observer warrants that, so far as that member/observer is aware, that IP does not infringe a third party's IP.

By contributing IP to an activity, the member/observer grants the Company an irrevocable, sub-licensable, non-exclusive, royalty-free worldwide licence to use or reproduce the IP or carry out any activity that would but for this licence infringe the field IP, in connection with a deliverable or the implementation of a deliverable.

For the avoidance of doubt, ownership of any original contribution of field IP is not assigned to the Company.

Confidentiality

Except as expressly provided below, all Activity shall be non-confidential, and all documents submitted in connection with an Activity by a member or observer, or affiliate of a member or observer shall be treated as non-confidential.

Information will be treated as confidential (“Confidential Information”) in the following circumstances:

- the confidential information is in written form, and the confidential information is clearly identified; and
- the information is identified as confidential in writing; and
- the confidential information, together with a request that it is treated as confidential has first been submitted to the Company, who has accepted that the information is confidential.

Confidential Information may be disclosed to any members/observers provided that the member/observer to whom the Confidential Information is disclosed is informed of the confidential nature of the Confidential Information before disclosure.

In the event that Confidential Information is to be discussed, referred to or otherwise used during an Activity, the Activity (or part thereof) shall be confidential only in so far as it is strictly necessary to maintain the confidentiality in the Confidential Information.

Any information that is treated as confidential pursuant to clause 11.2 that is incorporated into a Deliverable will be deemed to be non-confidential from the date upon which that Deliverable is issued.
Warranties

The Company makes no representations or gives any warranties as to non-infringement of Third-Party IP or Patents in relation to this IPR Policy.

The Company makes no representation or warranty as to the validity of any claim of any Field Patent, or as to the essentiality to a Standard of any claim of a Field Patent.

The member or observer agrees not to assert its Field IP or Field Patents against the Company in respect of any promotion or publication of Deliverables (including Standards) by the Company, during the period of its membership or afterwards.

If any member or observer breaches its obligations under this IPR Policy, the Company reserves the right to take any actions available to the Company under its procedures or at law, in order to protect the interests of the Company or of any other Member or Observer, including but not limited to excluding the defaulting member or observer from any Activities or terminating its membership.

The Company is not responsible for determining whether any proposed licensing terms are on FRAND Terms.

To the fullest extent permitted by law, the Company shall not be liable to the member or observer for any costs, expenses, loss or damage (whether direct, indirect or consequential, and whether economic or other) arising from the member or observer’s exercise of the rights granted to it under this IPR Policy.

Subject to the above, the total liability of the Company under or in connection with the IPR Policy (whether arising in contract, tort, negligence, breach of statutory duty or otherwise) shall not exceed the sum of the annual fee paid by the Member or Observer.
Financial Position
11 Financial Position

The Company’s accounts Financial Year ending 30 September 2018 were filed with Companies House in the United Kingdom on 9 April 2019.