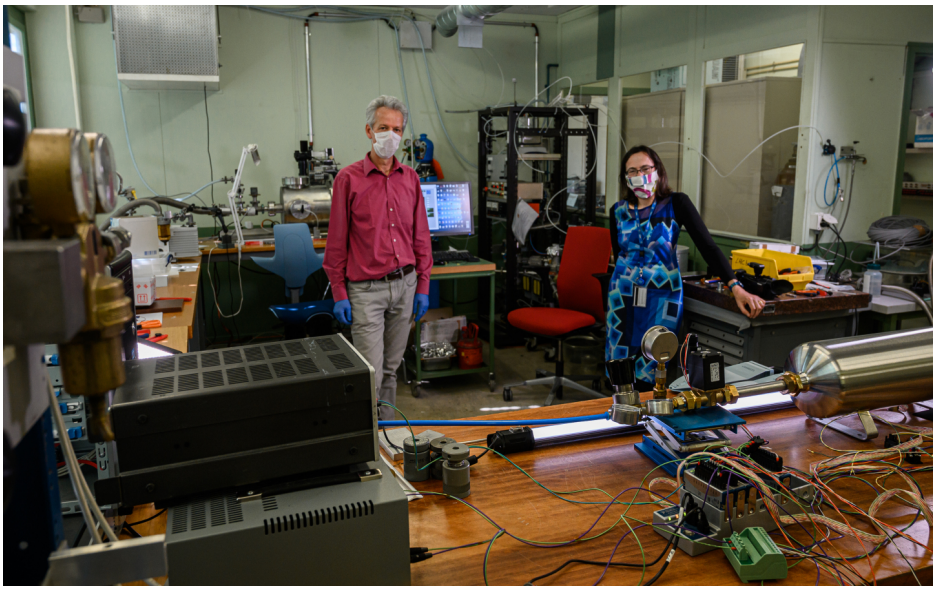
# CERN Bulletin

Issue No. 16-16/2020-Wednesday 08 April 2020
More articles at *http://home.cern/cern-people*


# INITIATIVES FROM THE CERN COMMUNITY IN GLOBAL FIGHT AGAINST COVID-19

**The "CERN against COVID-19" taskforce, which coordinates the actions, has received hundreds of suggestions to contribute to the efforts to curb the pandemic**



*Jan Buytaert and Paula Collins in their CERN laboratory where they develop the new HEV ventilator which prototype is visible in the foreground (Image: Jacques Fichet, Samuel Hertzog/CERN)*

Members of the CERN community have shown ingenuity and generosity in their contribution to the struggle against the COVID-19 pandemic. The "CERN against COVID-19" taskforce, which was established at the end of March to identify and support these initiatives, has already received hundreds of messages suggesting ideas ranging from producing sanitizer gel to designing and building sophisticated medical equipment. Indeed, CERN and its community can make use of important resources such as the Worldwide LHC Computing Grid, mechanical workshops, sophisticated design and prototyping facilities, advanced technologies and expertise ranging from science and engineering to industrialisation.

The taskforce was set up to ensure effective and well-coordinated action, working closely with experts in healthcare, drug development, epidemiology and emergency response so as to maximise the impact of the Organization's contributions. CERN has established links with local hospitals and emergency services, and in the context of an agreement established in 2011, entered into dialogue with experts at the World Health Organization.

*(Continued on page 2)*

## In this issue




**Published by:**
CERN-1211 Geneva 23, Switzerland writing-team@cern.ch
**Printed by:** CERN Printshop


CERN-ISSN: **Printed version:** 2011-950X
**Electronic Version:** 2077-9518

# INITIATIVES FROM THE CERN COMMUNITY IN GLOBAL FIGHT AGAINST COVID-19

Discussions are also underway with sister European scientific organisations, the European Molecular Biology Organization and the European Bioinformatics Institute.

“We have been very encouraged by the enthusiasm of the community to contribute,” said task-force chair Beniamino Di Girolamo, chair of the taskforce. “Ideas range from the deployment of CERN's powerful computing, engineering and technical resources, to assisting the local effort through logistical and emergency response support.”

Initiatives already underway include the production of one tonne of sanitizer gel to distribute to local emergency-response teams. The CERN Fire and Rescue Service has been working with the emergency services in the region since late March. CERN's 3D-printing and workshop capability has been deployed to complement the production of protective equipment such as masks and Perspex barriers for law enforcement in the region. Studies are underway to deploy the particle physics community's considerable computing capacity to assist in the search for a vaccine.

Another project being pursued is a novel streamlined ventilator, called HEV. A team of physicists and engineers from the LHCb collaboration at CERN led the initiative. They are supported by a number of CERN service. As the pandemic spreads, the number of hospitalised patients requiring ventilators has led to a global shortage of supplies. The team realised that the types of systems used to regulate gas flows for particle physics detectors could be used to design a novel ventilator. The HEV design could be used for patients in mild or recovery phases, enabling the more high-end machines to be freed up for the most intensive cases. It is a safety-first design, intended to satisfy clinical requirements for the most requested ventilation modes for COVID-19 patients.

The first stage of prototyping was achieved at CERN on 27 March, with a concept that relies on inexpensive and readily available components. The desired physical characteristics of the pressure regulators, valves and pressure sensors are now being refined, and the support of clinicians and international organisations is being harnessed for further testing within hospital settings. The control software for this device will be encapsulated in a dedicated microcontroller that will, along with other low-power components, enable the deployment of the HEV in areas with limited resources and unstable power distribution. This will allow it to be powered with batteries, solar panels or emergency power generators.

Two other groups of scientists are behind similar initiatives. One group in the Global Argon Dark Matter collaboration proposed a fan (called MVM) that uses components that are also readily available and could be produced rapidly on a large scale. A team from the Laboratory of Instrumentation and Experimental Particle Physics in Portugal, among others, has also presented a concept for a cost-effective ventilator (Open Air project) using a limited number of components.

The aim is to release CERN developments against COVID-19 under the CERN Open Hardware Licence so that equipment may be produced wherever there is a need, and adapted to local regulatory frameworks.

*Don't forget to read the* CERN Courier (*https://cerncourier.com/a/particle-physicists-propose-stripped-down-ventilator-to-help-combat-covid-19/*) *article about this issue.*

*Follow the progress of the initiatives on this site: cern.ch/against-covid-19.*

# RECORD NUMBER OF SUBMISSIONS FOR “BEAMLINE FOR SCHOOLS”

**Some of the 198 experiment proposals from high-school student teams will be carried out at a fully-equipped accelerator beamline**


*Winners of the 2019 Beamline for Schools competition work on their projects at DESY Hamburg (Image: CERN)*

The deadline for the seventh edition of the Beamline for Schools competition expired on 31 March 2020. An exceptionally high number of proposals has been received despite the current difficult situation worldwide. In total, 198 proposals from 47 countries have been submitted. Outside of the very first edition in 2014, this marks a new record! We thank the more than 1400 students worldwide for their motivation and engagement.

This year again, white spots on the world map could be filled with countries which have taken part in this competition for the very first time: Guatemala, Iraq, Kazakhstan, Nigeria, North Macedonia, Saudi Arabia, Taiwan and Tanzania. This confirms the international character of this competition. A total of 43% of all proposals are coming from CERN Member or Associated Member States and 57% from non-Member States. Furthermore, seven teams collaborated across borders and consisted of students from several countries each.

Since 2014, the Beamline for Schools competition invites teams of high-school students to propose a scientific experiment

that they want to perform. The teams behind the selected projects get to see it carried out at a fully-equipped accelerator beamline. Due to CERN's shutdown of its accelerators for maintenance and upgrade, the winning experiments in 2020 will be run at DESY in Hamburg, Germany in autumn.

Now that the submission phase is over, the evaluation process has started, with about 50 experts involved. Besides the two winning teams, we will also announce shortlisted teams winning extra prizes. The official press release announcing the winners of this year's BL4S competition will follow in June, so stay tuned!

---

*Beamline for Schools is an Education and Outreach project funded by the CERN and Society Foundation and supported by individual donors, foundations and companies. The 2020 competition is partly supported by the Wilhelm and Else Heraeus Foundation, with additional contributions from the Arconic Foundation and the Fund Ernest Solvay, managed by the King Baudouin Foundation.*

# TOMORROW IS ANOTHER DAY

**A video message from the Director for accelerators and technology**

In this period of unprecedented challenges in working at a distance from each other for most of us, we will regularly post video messages from members of the management teams on the website for the CERN Community.

The first message is from Frédérick Bordry, Director for Accelerators and Technology, who calls on us to show solidarity and looks forward to easier days.

This message was recorded on 31 March (*https://videos.cern.ch/record/2714421*).

# UPDATE OF THE EUROPEAN STRATEGY FOR PARTICLE PHYSICS POSTPONED

**The extraordinary session of the CERN Council scheduled for 25 May will be replaced by a discussion via videoconference to determine the next steps in the process**


*(Image: CERN)*

Due to the situation arising from the COVID-19 pandemic, the CERN Council has postponed the next step in the update of the European Strategy for Particle Physics. During a special session that was scheduled to take place in Budapest on 25 May, the Council was due to adopt and make public the recommendations made by the European Strategy Group during a drafting session in January. This session will be replaced by a videoconference meeting, during which the delegations will discuss how to proceed.

The process of updating the European Strategy for Particle Physics began in 2017 and aims to define the long-term goals of the discipline. Discussions are being led by a group chaired by Halina Abramowicz of the University of Tel Aviv and comprising a delegate from each of CERN's Member and Associate Member States, as well as directors and representatives of major institutes and organisations in Europe and invitees from outside Europe. Following a call for proposals at the end of 2018, the results of which formed the basis of discussions at a symposium in May 2019, which itself led to the drafting of a briefing book, the European Strategy Group met in January 2020 to issue its recommendations.

*Read also the article in the CERN Courier (https://cerncourier.com/a/european-strategy-update-postponed/).*

# JUST A FEW DAYS LEFT BEFORE SUBMISSIONS FOR THE “BACKGROUND CHALLENGE” CLOSE!

**Submit your best home office photos on the dedicated website before next Monday**

*Our colleague Ewa in her peaceful and quiet home office, as part of the “Background challenge” contest (Image: CERN)*

The “Background challenge” photo contest allows the community to come together in these stressful times, to share a little bit of the intimacy of our homes and hopefully have a good laugh. The principle is simple: take a selfie in your home office in front of the background that your colleagues see during your video calls, and upload it on the website. (*https://background-challenge.web.cern.ch/*)

For those who are still at CERN, a photo of you on your work place will do the job. Since this is CERN, creativity and eccentricity are of course very much appreciated.

Submissions for your pictures will close next Monday 13 April, so make sure not to miss out on the fun! A one-week long voting period will follow, where you'll be asked to choose your favourite background. The winners will be celebrated on CERN's social media channels (if they wish to), and rewarded with a CERN T-shirt.

# COMPUTER SECURITY: BLACKMAILING ACADEMIA: BACK TO PEN AND PAPER(?)

**In recent months, a worrying trend has been emerging fast: targeted organisation-wide ransomware attacks**

The *Bulletin* article entitled “Blackmailing Enterprises: You are Patient Zero” raised a series of questions: “What is the problem for CERN?”, “We are academia!”, “Why should we worry?”. Some answers can be found below.

Ransomware attacks usually consist of tricking the victim into installing software that will eventually encrypt the victim's computer (and any remote share or backup that the user has access to) and asking for money – the ransom – in order to unlock (decrypt) the files. Such attacks have been happening for years. However, in recent months, a worrying trend has been emerging fast: targeted organisation-wide ransomware attacks. These attacks are carried out by well-organised and well-funded criminal groups.

Ransomware attacks typically start via traditional infection vectors like phishing e-mails (“You are Patient Zero”). For targeted attacks against an entire organisation, it is also common for the attacker to focus on exposed services, like unpatched Web applications exposed to the public Internet. Once access has been gained on a single device inside the network, the attacker then focuses on silently spreading the intrusion internally in order to gain access to privileged accounts or central services. After gaining access, the attacker explores the network, reading e-mails, finding data troves, and once they know the organisation in depth, they craft a plan to cause the most panic, pain and operational disruption. It can take an average of two to three weeks for the attacker to be in a position to enter the final stage of the attack. With the right level of access and control, the attacker only has to effectively deploy the ransomware payload in a single damaging wave to as many machines as possible, covering end-user machines, central services (e-mail, web servers, etc.), shared file systems and of course, backups. This may sound complicated and costly, but automated tools increasingly perform most of the work and ransomware is currently an incredibly profitable business, allowing attacking groups to source the appropriate expertise and staffing.

As soon as the targeted organisation realises it has been attacked, a ransom note is issued. The goal is very simple: inflict maximum damage on the daily operations of the victim organisation, so that it sees no other option but to pay the ransom. Very often, the damage is total: no IT. At all. Back to pen and paper. And it works extremely well. When Carleton University was affected, it was quoted as saying “Our research is halted right now because all our computers are either shut down or infected”. Sadly, when confronted with such a situation, some victims feel the only effective option is to pay the ransom. This happened at the University of Calgary : “The decision was made to pay the ransom because we do world-class research here [. . . ] and we did not want to be in a position that we had exhausted the option to get people's potential life work back in the future if they came today and said, 'I'm encrypted, I can't get my files,'” said Dalgetty [vice-president of finances and services].

This was in 2016. The academic and research sector is clearly perceived as a viable market for attackers, and their tactics and malicious frameworks have drastically evolved since then. More than half of today's ransomware victims end up paying the ransom. Criminal organisations are taking the time to research their victims in order to maximise the potential damage to the organisation and their payoff. The amount for the ransom demanded is “just right”, basically the maximum amount that the organisation can afford to pay. The University of Maastricht was one of the rare victims to expose the attack publicly and even shared a detailed technical report. In

2016, the University of Calgary paid about 20 kCHF. But in 2019, the stakes are higher and the University of Maastricht agreed to pay around 230 kCHF in the hope of unlocking its systems. The attacker completely annihilated the University's computing and network infrastructure on 23 December, and the timing made the attack even more difficult to handle.

That said, a number of organisations seem to elect not to pay. They may acknowledge that it makes us all less safe, but most importantly that there is no guarantee the files will be unlocked by the criminals. Not all victims agree to share the figures, but ransomware attacks have such a profound impact on the core technical infrastructure of the victim that they are immensely costly, no matter the strategy. A recent example is a large steel producer that had to close 170 factories and offices when faced with paying a 380 kCHF ransom. They refused to pay and the recovery cost was estimated to be around 56 MCHF. The City of Baltimore also did not pay and "has put more than $18 million into the attack. The hackers originally demanded $76,000."

There are also massive hidden costs: the attacker has access to all of the organisation's data and information, including personal data about employees, customers, business partners and technologies. And it is hardly possible to hide or continue to operate during a successful ransomware attack, which itself brings additional, significant reputational damage. A ransomware infection must be considered a data breach until investigation proves otherwise. More and more of the ransomware operators are now leaking data belonging to victims who fail to pay up. This recent development means that organisations are increasingly likely to pay the ransom. The cyber insurance industry has also adapted to the new reality. It's getting more and more expensive to transfer the risk of ransomware, as underwriters are raising premiums for their coverage.

Over the course of the last months and even weeks, the number of victims in the academic sector has kept increasing, with a worrying trend of academic institutions paying ransoms, like Regis University in Denver. It would be too easy to blame the more open "academic environment" in which we operate our services. Our sector is not the only one affected: some serious industry actors are victims as well. One example is Travelex, whose entire banking system was taken down globally after an attack on New Year's Eve. "Travelex cashiers have been resorting to using pen and paper to keep money moving at cash desks in airports and on the high street." Beside the attack's operational costs, the damage to Travelex's business and reputation is of course gigantic, forcing its CEO to read a public statement regarding the attack. In another attack in December 2019, a US Coast Guard base was taken offline for 30 hours as "ransomware interrupted cameras, door-access control systems and critical monitoring systems at the site".

Recently, ransomware started adding additional functionality to target Industrial Control Systems operations. If such ransomware were to make its way into the CERN Technical Network, that could pose significant risks for the operation of the accelerator complex and the experiments. Even if the malware does not spread to actual programmable logic controllers (PLCs), it can still halt the operations of complex industrial equipment: "[The] natural gas facility shut down operations for two days after sustaining a ransomware infection", as "A cyber threat actor used a Spearphishing Link to obtain initial access to the organisation's information technology (IT) network before pivoting to its OT network. The threat actor then deployed commodity ransomware to encrypt data for impact on both networks." The situation is certainly not new, but the number of victims is rapidly increasing. And most importantly, the fact that the attackers take the time needed and have the capabilities to deploy ransomware so deeply in the victims' computing and network infrastructure is a new development.

On behalf of the Swiss Government, MELANI has issued multiple advisories and repeated warnings specifically on this issue, as "several well-known Swiss companies have been affected by this kind of attack". In the same vein, the French ANSSI also produced a detailed report, and explicitly warn that organisation-wide ransomware is currently the most serious computing threat for institutions and companies. ANSSI add that such attacks are sometimes as sophisticated as nation-state sponsored espionage operations. As a result, the question is not whether well-funded organised groups will target CERN with an organisation-wide ransomware attack, but when. But the most important question is: what do we do about it?

- Phishing detection: Our anti-malware filtering appliances detect most phishing e-mails, in particular those containing attachments. But this does not provide complete protection: it is in particular quite weak against embedded links, which are not monitored by the security system in order to protect the privacy of users. Due to this configuration, it is easy to insert a malicious download link in an e-mail, and it remains reasonably simple to successfully send a malicious attachment.
- Security patching of exposed services: It is absolutely crucial to keep all exposed services fully patched. More and more malware carries out scans of the local network even after the initial infection in order to propagate inside the organisation. An example is Emotet, which often delivers the Trickbot ransomware as a second stage. A leading university was affected by an organisation-wide ransomware attack after the attacker "manually" compromised an unpatched Web application after scanning and exploring their exposed services. It is common to have delayed security patching on non-critical services – these make easy targets for attacking groups.
- End-point protection: The current signature-based protection unfortunately has a low malware detection rate. Efforts towards better "Endpoint Detection and Response" are ongoing by IT-CDA, although there is no defined timeline or budget.
- Threat intelligence / SOC: The CERN Computer Security Team takes great care to collect known ransomware "command and control" servers from hundreds of partners, including MELANI and other government agencies. Very often this provides after-the-fact response capabilities, and does not guarantee all ransomware attacks will be detected.

After the attack, the University of Maastricht produced a number of recommendations based on the lessons it learnt, most of which are relevant to CERN as well. Basically, resilience is the key. It is absolutely crucial to keep all exposed services fully patched. You can help the Organization with that by keeping your computer, laptop, smartphone and, if you manage one, computing service up-to-date. Make sure that you have appropriate back-ups that are not susceptible to unintentional modification or deletion. Secure your computing account appropriately, do not disclose your password to

third parties, and segregate the power of service accounts so that the exposure of one does not compromise all the systems you manage. Finally, STOP – THINK – DON'T CLICK on unknown attachments or weblinks, so you don't become the patient zero compromising CERN (see our *Bulletin* article entitled “Blackmailing Enterprises: You are Patient Zero”).

---

*Do you want to learn more about computer security incidents and issues at CERN? Follow our Monthly Report. For further information, questions or help, check our website or contact us at Computer.Security@cern.ch.*


*This is the one phishing e-mail it took to bring the entire computing infrastructure of University of Maastricht down.*

*The Computer Security Team*

# Official communications

## TRAVEL WITHIN AND ENTRY INTO FRANCE

Travel within France is authorised only under the conditions set out in this document (*https://www.interieur.gouv.fr/fr/Actualites/L-actu-du-Ministere/Attestation-de-deplacement-derogatoire-et-justificatif-de-deplacement-professionnel*). In order to travel, you must have a certificate of special dispensation (*attestation de déplacement dérogatoire*) in your possession. This certificate may be generated electronically (to be shown on a smartphone or tablet) or completed on paper (printed out or hand-written). A new certificate must be used for each day and for each activity. You must also carry an identity document. Without these, you are liable to be fined.

For professional travel (i.e. between your home and place of work), a certificate issued by CERN is also required in addition to the certificate of special dispensation.

A new certificate of special dispensation came into force on 8 April 2020 for entry into France from another country or travel between mainland France and its overseas territories.

Please note that this certificate is not required if you are travelling between Switzerland and neighbouring France (Ain and Haute-Savoie) for professional reasons and you are in possession of the above-mentioned CERN certificate, which is issued to individuals called upon to “travel between their home and CERN's installations located in Switzerland and France, for the purpose of essential activities to ensure the safety and security of the Organization's site and equipment”.

See also the information on the website of the French interior ministry regarding electronic and downloadable certificates (*https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Attestation-de-deplacement-derogatoire-et-justificatif-de-deplacement-professionnel*).

*Relations with the Host States Service*

## MEASURES FOR ENTRY AND MEDICAL TREATMENT IN SWITZERLAND

Due to the COVID-19 pandemic, the Swiss authorities have restricted entry into Switzerland. Only Swiss citizens, holders of a residence permit in Switzerland (including a FDFA legitimation card), and persons with a certified professional reason for entering Switzerland may enter the country.

Non-Swiss citizens and persons not holding a valid Swiss resident permit may not, in principle, travel to Switzerland to receive medical treatment.

However, exceptions may be granted in particular when a person is in a situation of absolute necessity. The continuation of a medical treatment that has begun in Switzerland and cannot be postponed without endangering the patient's life is one of the grounds for absolute necessity, as stated in the Directive of the State Secretariat for Migration (*https://www.sem.admin.ch/content/dam/data/sem/aktuell/aktuell/einreisestopp/weisung-covid-19-f.pdf*).

The person concerned must therefore be able to present, when crossing the border, a certificate issued and signed by the Swiss treating doctor stating that the patient must imperatively continue their medical treatment which cannot be postponed without endangering their life and indicating the date on which the medical treatment began in Switzerland.

In order to facilitate the crossing of the border, the person must send a prior request by e-mail to the Swiss Mission (geneve.visa@eda.admin.ch). This request must be accompanied by documentary evidence and indicate the planned point of entry into Switzerland. This will enable the

Swiss Mission where applicable to authorise the person's entry into Switzerland and to notify the relevant border post accordingly in advance.

The Host State Relations service (relations.secretariat@cern.ch) is at the disposal for any question prior to the process of contacting the Swiss Mission.

*Host States Relations service*

# TAXATION IN FRANCE

### Memorandum concerning the annual certificates 2019 and the declaration of income for 2019 in France

The Organization would like to remind members of the personnel that they must comply with the national legislation applicable to them, in particular for any other income they may receive from sources other than CERN (cf. Article S V 2.02 of the Staff Rules).

I - Annual internal taxation certificate and financial certificate for 2019

Depending on your status at CERN in 2019, the annual internal taxation certificate or the financial certificate for 2019, issued by Finance and Administrative Processes Department, is available since 7 February 2020 via HRT (*http://hrt.cern.ch/*) (under “My e-Documents and Self Services”). It is intended exclusively for the tax authorities.

1. If you are currently a member of the CERN personnel, you will have received an e-mail containing a link to your annual certificate, which you can print out if necessary.
2. If you are no longer a member of the CERN personnel or are unable to access your annual certificate as indicated above, you will find information explaining how to obtain one on this page (*https://admin-eguide.web.cern.ch/en/procedure/annual-certificates*).

In case of difficulty in obtaining your annual certificate, send an e-mail explaining the problem to service-desk@cern.ch.

II - 2019 income tax declaration form in France

The 2019 income tax declaration form must be completed following the general indications available on this page (*https://admin-eguide.web.cern.ch/en/procedure/income-tax-declaration-france*).

**IF YOU HAVE ANY SPECIFIC QUESTIONS, PLEASE CONTACT YOUR LOCAL “*SERVICE DES IMPÔTS DES PARTICULIERS*” (SIP, PRIVATE CITIZENS' TAX OFFICE) DIRECTLY.**

This information does not concern CERN pensioners, as they are no longer members of the CERN personnel and are therefore subject to the standard national legal provisions relating to taxation.

*HR Department*
*HR-Internal-tax@cern.ch*

*Human Resources Department*

# TAX DECLARATION: FOR THE ATTENTION OF MEMBERS OF THE PERSONNEL AND PENSIONERS LIVING IN FRANCE

### Exchange rate for 2019

For 2019, the average annual exchange rate is **EUR 0.90 for CHF 1**.

*Human Resources Department*

# Announcements

## ACCESS CARDS VALIDITY EXTENDED

**In order to avoid any problems with expiring access cards during stage 3, CERN has taken the exceptional decision to extend the access cards validity by 6 months**

In order to avoid any problems with expiring access cards during Stage 3, CERN has taken the exceptional decision to extend the access cards validity by 6 months.

All personnel concerned will receive an e-mail with the necessary information.

If you are currently in a position to come to CERN on a normal working day, please note that Building 55 is open as usual (see services availability) and that you can have your card renewed straight away.

*SMB and BE Departments*

## SUPPORT AGAINST ISOLATION

**CERN can provide some support if you feel isolated and need it**

CERN can provide some support if you feel isolated and need it.

Detailed anti-isolation support provided by HR can be found in the leaflet on this link.

Further, you can contact the helpline COVID-19 at +41 22 766 77 77 or the Medical Service at +41 22 767 31 86 / medical.service@cern.ch, or get support from the CERN psychologist, Christiane Reis.

Appointments with the CERN psychologist can be taken via the CERN Medical Service: medical.service@cern.ch.

## DURATION OF STAGE 3

**Stage 3, and the measures that are implemented as part of this stage for all our members of personnel, last until further notice**

CERN has entered the fourth week of Stage 3 of the COVID-19 response. On-site activities are limited to those essential for the safety and security of the site and equipment, and many colleagues are teleworking. Stage 3, and the measures that are implemented as part of this stage for all our members of personnel, last until further notice.

For questions related to teleworking or absences, members of personnel should contact their supervisor directly to discuss their personal situation. As we learn to adapt to this exceptional situation, it is important that we stay connected. Information to our community will be updated through the COVID-19 information webpage and the usual communication channels, such as the CERN Bulletin, which is now published weekly.

To date, CERN has information of ten members of its personnel having tested positive for coronavirus (COVID-19), of which two are currently not in the local area. Whenever CERN is informed of a tested or suspected case, we follow the evolution of the concerned individuals' health closely. We also apply procedures to quickly identify the individuals' close professional on-site contacts (if any) in order to ensure their well-being and self-quarantine, with a view to safeguarding their health, as well as that of the communities they are in. The number of CERN members of personnel confirmed to have been diagnosed with COVID-19 will be updated weekly.

For up-to-date information, please see: https://hse.cern/news-article/coronavirus-recommendations.

*The COVID-19 response team*

# EXPLORE CERN'S WEALTH OF RESOURCES #2

**The CERN community is not short of resources... and now is the ideal time to take advantage of them!**

*The ATLAS Colouring Book, a resource for the younger ones (Image: CERN)*

The CERN community is not short of resources... and now is the ideal time to take advantage of them! Here are some new ideas for activities that can entertain, inform or educate during lockdown.

- The Education, Communication and Outreach group has compiled a list of resources to discover CERN online (*http://visit.cern/discover-cern-online*) from the comfort of your home: activities for children, virtual tours and a selection of videos about the Laboratory!

- The Library makes more than 94,000 ebooks available to the CERN community. A complete list of the resources available has been compiled here (*http://library.web.cern.ch/online-resources-available-cern-users-during-covid-19-epidemics*).

For more ideas, consult Explore CERN's wealth of resources #1 (*https://home.cern/news/announcement/cern/explore-cerns-wealth-resources-1*).

———

*If you would like to share other CERN resources or initiatives with the community, don't hesitate to contact us at writing-team@cern.ch.*

# READ EBOOKS DURING ACCESS RESTRICTIONS

**The Library makes more than 94,000 ebooks available to the CERN community!**

The easiest way to access them is to search on the CERN Document Server (CDS) in our ebooks collection (*https://cds.cern.ch/collection/eBooks*).

Once you have found the book(s) you would like to read, simply click on the 'ebook' link below the book description. If you are not already logged in, you will be asked to do so. Then, depending on the ebook, you will be redirected either on:

- The publisher's website: where you can access and download the ebook.
- *O'Reilly* website: where you can read online the ebook. Choose CERN in 'Select your institution'.
- *Ebook Central* website: where you can either read online/download the ebook, or 'request' access to the ebook. In the case of a request, please fill in the form and we will answer you as soon as possible.

Some publishers have also decided to open some of their resources during the epidemics, **a complete list of the resources available for the CERN community** has been compiled here (*http://library.web.cern.ch/online-resources-available-cern-users-during-covid-19-epidemics*). If you do not go through CDS but come across an ebook directly on the web and it is behind a paywall, you can check if we have access to it by adding the prefix: *http://ezproxy.cern.ch/login?url=* at the beginning of the URL and then reload the page.

If you still cannot access the ebook after that, it probably means that we do not have access to it; in this case, you can contact us (see below). Here you can find more information about the remote access to our e-resources (*http://library.cern/resources/remote*).
If you do not find the book you are looking for on CDS or cannot access an ebook you would like to read, please contact us by email: library.desk@cern.ch (*http://library.desk@cern.ch*) or via Mattermost (*https://mattermost.web.cern.ch/sis-team/channels/library-requests*).

*CERN Library*

# Ombud's corner

## SOLIDARITY IN THE TIME OF CORONAVIRUS

The whole world is experiencing a situation of a severity rarely seen, which is generating a great deal of anxiety and uncertainty. As in any time of crisis, initiatives to support others and promote solidarity are springing up everywhere, both in the professional world and in society in general.

I've been in touch by phone with several teams at CERN and have noticed that a great deal of effort is going into showing understanding and kindness towards others to combat the effects of isolation and confinement. I thought that you would be interested and inspired to hear about what some of your colleagues at CERN are doing.

Firstly, most teams have continued with their regular meetings, except that now they are held remotely, and some teams have even increased their frequency. Those who are particularly susceptible to the effects of physical distancing and isolation are regularly receiving calls from their supervisors or colleagues. Some supervisors are making it a point of honour to call every member of their team at least once a day. Others who are in charge of larger teams regularly send a personal message to each team member via e-mail. All of this takes time and energy, but it shows the importance that is being attached to solidarity in these particularly trying times.

We are also seeing that people are more reactive than usual: colleagues seem to be keen to respond quickly to requests so as not to drag things out unnecessarily.

Phone calls and videoconferencing are more popular than ever: what could be nicer than being able to have a conversation with your colleague rather than exchanging dozens of e-mails! These contacts are primarily professional, but they have also become more personal: we want to know how everyone is coping with the situation, and sometimes we even get to meet the children of our colleagues, or their spouse, their cat, their dog...

And then there are the less formal initiatives, like the organisation of regular "video coffee breaks" to fill the gap left by the absence of the informal encounters that are so vital to office life. Many colleagues now sign off their messages with a little touch of humour, a funny picture or a video, to keep people's spirits up. Some clubs are even continuing their activities or classes via videoconference.

We are living through a difficult time, but as a result many people are taking steps to help one another, to be creative and to show solidarity. No-one really knows how long the lockdown will last, so we must be mentally prepared to continue these efforts.

Don't forget that all the usual support services remain at your disposal, albeit remotely. Don't hesitate to use them! Now, more than ever, we are all available to help and advise you.

*Pierre Gildemyn*

*If you'd like to comment on any of my articles or suggest a topic that I could write about, please don't hesitate to e-mail me at Ombuds@cern.ch .*