

# راهنمای امنیت زیستی کاربردی برای آزمایشگاه‌های علوم زیستی

پیتر کله وستینگ و علی کرمی



## بنیاد پژوهش‌های صلح جهانی در استکهلم

بنیاد پژوهش‌های صلح جهانی استکهلم (SIPRI) یک بنیاد جهانی غیر وابسته و پژوهشی در حوزه مسائل صلح و مناقشه، به‌ویژه در زمینه نظارت بر تسلیحات و خلع سلاح است. این بنیاد، در سال ۱۹۶۶ در سوئد تاسیس شد، آمار، اطلاعات، تجزیه و تحلیل‌های در SIPRI براساس سیاست‌های منبع باز به سیاست‌گذاران، محققان، رسانه‌ها و عامه مردم علاقه‌مند ارائه شده است.

## هیئت مدیره بنیاد پژوهش‌های صلح جهانی استکهلم، عبارتند از:

یوران لینمارکر Göran Lennmarker، رییس هیات مدیره (سوئد)

دکتر دوی فورتونا انوار Dewi Fortuna Anwar (اندونزیا)

دکتر ولادیمیر بارانوسکی Vladimir Baranovsky (روسیه)

سفیر لاخدار براهیمی Lakhdar Brahimi (الجزایر)

جایانتا داناپالا Jayantha Dhanapala (سری لانکا)

سوزان آیزنهاور Susan Eisenhower (ایالات متحده)

سفیر ولفگانگ ایشینگر Wolfgang Ischinger (آلمان)

پروفسور ماری کالدور Mary Kaldor (انگلستان)

**مدیرعامل:** دکتر بیتس گیل Bates Gill، (ایالات متحده)



**STOCKHOLM INTERNATIONAL  
PEACE RESEARCH INSTITUTE**

Signalistgatan 9

SE-169 70 Solna, Sweden

Telephone: +46 8 655 97 00

Fax: +46 8 655 97 33

Email: sipri@sipri.org

Internet: www.sipri.org

# راهنمای امنیت زیستی کاربردی برای آزمایشگاه‌های علوم زیستی

بیتر کله وستینگ و علی کرمی



STOCKHOLM INTERNATIONAL  
PEACE RESEARCH INSTITUTE

۲۰۱۲

© SIPRI 2012

همه حقوق محفوظ است. تکثیر، ذخیره‌سازی در دستگاه‌های بازیابی یا مخابره این نوشته به هر شکل و هر وسیله‌ای بدون کسب اجازه کتبی قبلی از SIPRI و به جز مواردی که قانون به صراحت مجاز می‌شمارد، ممنوع است.

عکس‌ها اهدایی سازمان کنترل و پیشگیری بیماری (CDC) همچنین می‌توانید نسخه اصلی را از طریق وب سایت رسمی SIPRI دریافت نمایید. ([www.sipri.org](http://www.sipri.org))

ISBN 978-91-85114-68-9



## فهرست مطالب

### پیشگفتار

iv

### ۱- هدف این راهنما

۱

### ۲- اجزای امنیت زیستی کاربردی

۳

۲.۱. امنیت زیستی - کاربردی چیست؟

۳

۲.۲. برآورد خطر در امنیت زیستی

۴

۲.۳. امنیت زیستی - کاربردی در عمل

۶

۲.۳.۱. پاسخگویی کارمندان

۷

۲.۳.۲. کنترل مواد

۸

۲.۳.۳. حفاظت فیزیکی

۹

۲.۳.۴. حفاظت اطلاعات

۱۲

۲.۳.۵. امنیت جابه‌جایی و حمل و نقل

۱۳

### ۳- سرپرستی امنیت زیستی - کاربردی

۱۶

۳.۱. نکات مورد توجه مدیر آزمایشگاه و سرمحقق در امور امنیت زیستی

۱۶

۳.۲. مدیریت امنیت زیستی کاربردی

۱۶

۳.۲.۱. مدیریت مواد

۱۷

۳.۲.۲. مدیریت کارکنان

۱۸

۳.۲.۳. مدیریت اطلاعات

۲۰

۳.۳. فوریت‌های امنیت زیستی

۲۲

۳.۳.۱. برنامه‌ریزی واکنش

۲۲

۳.۳.۲. گزارش نقض امنیت یا رخداد‌های امنیتی

۲۳

۳.۴. تمرین و ارزیابی

۲۳

### واژه‌نامه

۲۴

### پی‌نوشت‌ها

۲۶

### درباره نویسنده

۲۹



## پیشگفتار

هدف امنیت زیستی Biosecurity عبارت است از کاهش خطر سرقت، گم شدن، آلودگی عمدی و سرایت دادن بیماری‌ها و سموم. ایمنی زیستی Biosafety برای حفاظت از محیط زیست و ایمنی محل کار در جامعه پژوهشگران جا افتاده‌است، اما آگاهی از چگونگی سوءاستفاده‌های مغرضانه از علوم زیستی هنوز چندان گسترده نیست. ارسال پاکت‌هایی حاوی اسپور سیاه‌زخم از سوی فرستندگان ناشناس به سیاستمداران و کارکنان رسانه‌ها آن‌هم از طریق پست آمریکا در سال ۲۰۰۱ توجه همه را به این نکته جلب کرد که دسترسی به امکانات علمی پیشرفته می‌تواند مورد سوءاستفاده نیز قرار بگیرد.

باعث افتخار بنیاد SIPRI است که نسخه ترجمه‌ای فارسی از کتاب راهنمای امنیت زیستی برای آزمایشگاه‌های علوم زیستی را در اختیار فارسی‌زبان قرار می‌دهد. نسخه اصلی این راهنما در سال ۲۰۰۹ منتشر گردید. در این راهنما اجزای اصلی امنیت زیستی - کاربردی مناسب برای همه کارکنان آزمایشگاه‌ها مطرح می‌شود. دولت‌ها و نهادهای گوناگون جهانی مشغول چاره‌اندیشی برای ایجاد موانعی بر سر راه خطر تروریسم بیولوژیک هستند و این راهنما تا عملی شدن آن اقدامات خلاء موجود را پر می‌کند.

نویسنده کتاب، دکتر پتر کلهوستیگ Peter Clevestig، ویروس‌شناس با تجربه همراه با دکتر علی کرمی، متخصص در بیوتکنولوژی پزشکی اقدام به ترجمه این راهنما نمودند. تشکر فراوان از هر دوی آنها برای کار حرفه‌ای و به‌موقع. تشکر فراوان سیپری از آژانس سوانح غیر نظامی سوئد (MSB)، با نام پیشین اداره مدیریت فوریت‌های سوئد، (KBM) که با کمک مالی خود انتشار این نوشته را ممکن ساختند و همچنین شرکت کارنگی (Carnegie) در نیویورک که حمایت مالی خود را از این ترجمه نمودند.

مایلم از سرپرستان پژوهشی این کار نوآورانه، دکتر ماریکا هلکوویست گرهبگ Marika Hellqvist Greberg و دکتر یان بیمان Jan Byman نیز تشکر کنم. همچنین سپاسگزارم از دکتر اوسا ژکلی بیورندال Åsa Szekely Björndal سرپرست اداره ایمنی زیستی سازمان پیشگیری از بیماری‌های واگیردار سوئد (SMI)، دکتر بریتا هگستروم Britta Häggström و دکتر اوکه فورشبرگ Åke Forsberg در سازمان پژوهش‌های دفاعی سوئد (FOI)، پروفسور رولاند مولبی Roland Möllby رئیس کمیته ایمنی زیستی بنیاد کارولینسکا، فریدا کولانو Frida Kuhlau در مرکز پژوهش‌های اخلاق و اخلاق زیستی دانشگاه اوپسالا، دکتر ایان آنتونی Ian Anthony مدیر پژوهش‌های سیپری و جان هارت John Hart رئیس پروژه ایمنی شیمیایی و بیولوژیک سیپری، برای پشتیبانی و راهنمایی‌های تخصصی آنها.

دکتر بیتس گیل Bates Gill

مدیر سیپری

ژوئن ۲۰۱۲



## ۱- هدف این راهنما

امنیت زیستی یا امنیت زیستی کاربردی، از اصول، فنون و اقداماتی سخن می‌گوید که برای حفاظت از پاتوژن‌ها، سموم، و فناوری‌های حساس، در برابر دسترسی غیر مجاز، گمشدن، به سرقت رفتن، و اشاعه عمدی یا سهوی اجرا می‌شوند.<sup>[۱]</sup>

راهنمای حاضر، در درجه نخست برای کارکنانی در نظر گرفته شده که با بیماری‌های واگیردار و سم‌هایی سروکار دارند که بهداشت و سلامت انسان‌ها، حیوانات و گیاهان را به خطر می‌اندازند. کار با مواد سمی در بخش‌های دولتی، هم‌چون دانشگاه‌ها، آموزشگاه‌های بهداشت یا دامپزشکی‌ها، آزمایشگاه‌های تحقیقاتی و تشخیصی) یا در بخش خصوصی بنگاه‌های صنایع زیستی و شرکت‌های داروسازی) صورت می‌گیرد. هدف این راهنما عبارت است از:

- علاقه‌مند کردن دانشمندان، کارکنان آزمایشگاه‌ها و دانشجویان به امنیت زیستی
- ارائه راهنمایی‌های عملی که کار مدیریت و نگهداری ایمن مواد بیولوژیک را تضمین می‌کند.

مقررات حاکم بر کنترل عوامل بیماری‌های واگیردار به‌طور عمده به‌منظور ایمنی کارکنان مراکز یادشده وضع شده است. این مقررات بیشتر در قوانین کشوری ناظر بر محیط و بهداشت کار ادغام شده است.<sup>[۲]</sup> نکات امنیتی کار در آزمایشگاه‌هایی که با عوامل بیماری‌های واگیردار سروکار دارند، اغلب نادیده گرفته می‌شود، مگر آنکه نکته‌ای مربوط به ایمنی زیستی نیز در میان باشد. به تازگی شماری رهنمود جهانی، راه‌های تجربی و آئین‌نامه منتشر شده است که در مجموع چهارچوبی را برای ایجاد استاندارد و کاربرد امنیت زیستی فراهم می‌سازند.<sup>[۳]</sup> با این همه راهنماهای کتبی کمی در زمینه امنیت زیستی - کاربردی برای استفاده کارکنان آزمایشگاه‌ها وجود دارد. اتحادیه اروپا (EU) سرگرم تهیه دستورالعمل‌های تازه‌ای در زمینه امنیت زیستی و نکات امنیتی مربوط به کار با عوامل بیماری‌های عفونی و سموم است.

اندکی پس از سال ۲۰۱۰ این دستورالعمل‌ها به‌عنوان پایه ایجاد قوانین کشوری ناظر بر آزمایشگاه‌ها به کار خواهند رفت. راهنمای حاضر می‌خواهد با تشویق دانشمندان، کارکنان آزمایشگاه‌ها، دانشجویان و مدیران به پذیرش رعایت امنیت به‌عنوان یکی از وجوه پراهمیت کار آزمایشگاهی، راه‌گذار به این قوانین را هموار سازد.

امنیت زیستی ایجاب می‌کند که هر یک از کارکنان درک کنند که هرگونه کار با بیماری‌های عفونی و سمی به‌خودی‌خود در بردارنده خطر امنیتی است: سلامت هر فرد نیز بالاترین ارزش را برای وی، آزمایشگاه و جامعه دارد و به همین دلیل در قبال آن وظایفی دارد. باور داشتن به



خطرهای امنیت زیستی و نقش مهم کارکنان، نکته حیاتی در حفظ ایمنی و امنیت محل کار است.

در قطعنامه شماره ۱۵۴۰ شورای امنیت سازمان ملل متحد و کنوانسیون سلاح‌های بیولوژیک و سمی (BTWC) به تاریخ ۱۹۷۲ نیز کنترل عوامل بیماری‌های واگیردار به عنوان یک وظیفه ملی و قانونی شمرده شده است.<sup>[۴]</sup>

بخش دوم این راهنما اجزای اصلی امنیت زیستی آزمایشگاهی را مطرح می‌کند که برای همه کارکنان آزمایشگاه‌ها کاربرد دارند. بخش سوم در درجه نخست برای مدیران و سرپرستان پژوهش‌ها در نظر گرفته شده است که نقش تصمیم‌گیرنده و مسئولیت‌اداری کارکنان و تعیین نقش آنان در آزمایشگاه را برعهده دارند در نظر گرفته شده است. تأکید این بخش بر نقش مدیران در حراست از اموال آزمایشگاه، شامل ذخایر انسانی است.



## ۲- اجزای امنیت زیستی کاربردی

### ۲.۱. امنیت زیستی - کاربردی چیست؟

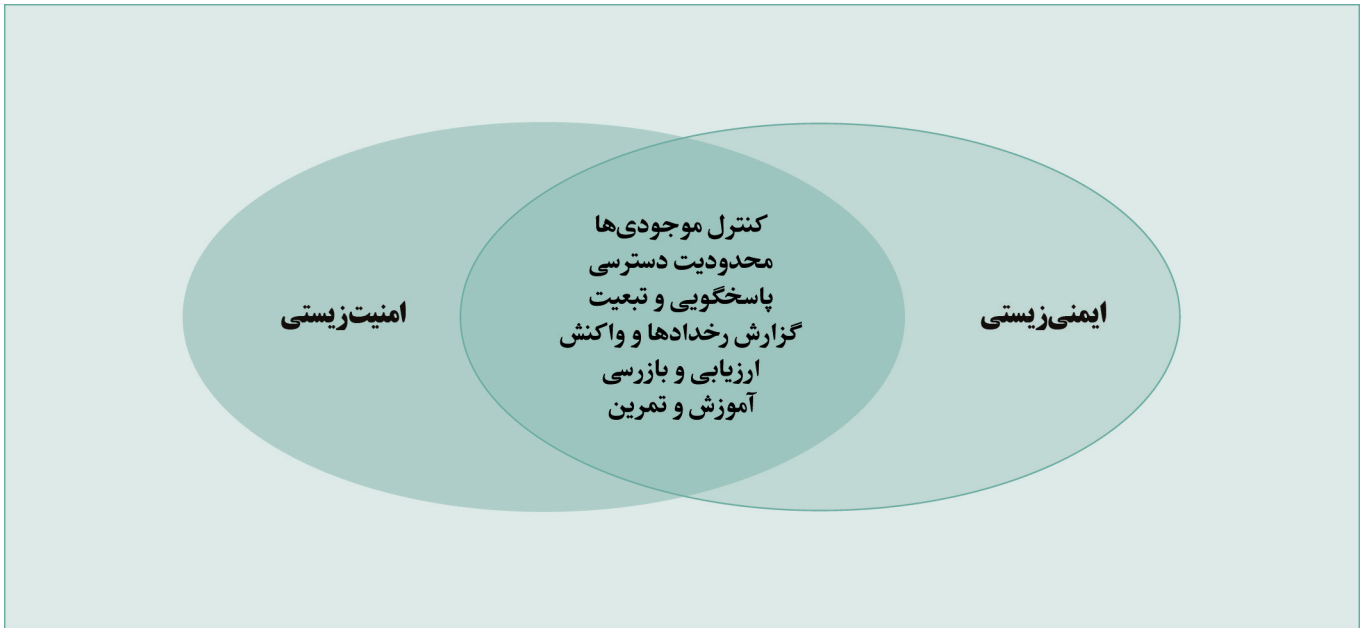
امنیت زیستی، طیف گسترده‌ای از خطرهای بالقوه را مورد بحث قرار می‌دهد که اقدامات بزهکاری‌های چون خرابکاری، تهاجم فردی و تروریسم بیولوژیک و جاسوسی را در بر می‌گیرد. اصطلاح «امنیت زیستی» در بحث‌های مربوط به خطر کاربردهای دوگانه علوم زیستی مطرح شده است. یعنی هنگامی که نتایج یک پژوهش قانونی، ممکن است با نیت تخریبی و بیرون از کاربرد مورد نظر اولیه به کار رود. اصطلاح «امنیت زیستی» برای خطرهای آلودگی محیط زیست و موارد مربوط به حفاظت از کشاورزی، مواد غذایی و دامی نیز به کار می‌رود. همچنین از آن در بحث پیرامون مهندسی ژنتیک به هنگام تولید و عرضه ارگانیسم‌هایی با ژن‌های دستکاری شده، یا گونه‌های مهاجم و بیگانه نیز استفاده می‌شود.<sup>[۵]</sup>

راهنمای حاضر روی کارهای آزمایشگاهی متمرکز شده است. در اینجا امنیت زیستی آزمایشگاهی از اصول، فنون و اقداماتی سخن می‌گوید که برای حفاظت از عوامل بیماری‌های عفونی و پاتوژن‌ها، سمها و اطلاعات حساس فنی در برابر دسترسی غیر مجاز، گم شدن، به سرقت رفتن، استفاده نابه‌جا و اشاعه عمدی یا سهوی اجرا می‌شوند.

هدف امنیت زیستی آزمایشگاهی عبارت است از حراست از مواد، کارکنان، اطلاعات و دیگر اموال آزمایشگاه، صرف نظر از این که کار آزمایشگاه در زمینه تحقیق است یا تشخیص بیماری، تولید دارو یا دیگر زمینه‌های علوم زیستی.

امنیت زیستی - کاربردی، خطرهای موجود در آزمایشگاه و تهدیدهایی را مورد توجه قرار می‌دهد که خارج از چهارچوب آلودگی اتفاقی فرد به عوامل بیماری‌زا قرار دارند. امنیت زیستی - کاربردی بر پایه زیست ایمنی شکل می‌گیرد و اجزای مشترک بسیاری با آن دارد. (شکل شماره ۱)

خطرهای امنیتی آزمایشگاه را در عمل با شناسایی اموال آزمایشگاه، از قبیل مواد بیولوژیک، اطلاعات و تجهیزات حساس، و با کسب اطمینان از امنیت این اموال و دانستن جایگاه و میزان هر کدام و نیز با ایجاد هشدار امنیتی می‌توان به حداقل رسانید. چنین رویکردی به سود کارکنان آزمایشگاه است و به عموم اطمینان می‌دهد که مواد بیولوژیک و کارهای مربوط به آن هم از ایمنی و هم از امنیت برخوردار است.



شکل شماره ۱. ارتباط میان ایمنی زیستی و امنیت زیستی  
 ایمنی زیستی و امنیت زیستی هر دو رویکردی‌هایی برای تأمین حفاظت و هر دو در خدمت رسیدن به هدفی مشترک هستند که عبارت است از به حداقل رساندن آلودگی یا سرایت اتفاقی یا عمدی پاتوژن‌ها یا سموم. برخی اجزای این دو نیز مشترک است؛ از قبیل کنترل موجودی‌ها، محدودیت دسترسی، پاسخگویی و تبعیت، گزارش رخدادها، ارزیابی و بازرسی، و آموزش و تمرین.

### ۲.۲. برآورد خطر در امنیت زیستی

با برآورد خطر می‌توان میزان خطر ناشی از هر یک از عملیات آزمایشگاه را سنجید. میزان خطر متناسب است با میزان احتمال رخ دادن یک حادثه و پی‌آمدهای آن. (شکل شماره ۲)<sup>[۶]</sup> کار کردن با هر پاتوژن یا سم در بردارنده خطرهای زیست ایمنی است، اما شدت آسیبی که عوامل بیماری‌زا یا سموم در پی دارند، متفاوت است.

هدف روش‌های سنجش ایمنی، نگاه داشتن خطر در سطح ایمن است. برخی از این روش‌های ایمنی عبارت هستند از داشتن تجربه کافی در کار آزمایشگاهی و به‌کار بستن تجهیزات و روش‌های ایمن، شامل اتاقک‌ها یا هودهای ایمن، تجهیزات حفاظت شخصی و تکنیک‌های درست آلودگی‌زدایی پس از کار.<sup>[۷]</sup>

برخی کشورها مقررات محیط کار را برای کاهش خطرات کار با عوامل بیماری‌های عفونی و سموم به کار می‌بندند.<sup>[۸]</sup>

گذشته از خطرهای آلودگی اتفاقی و بیماری‌های ناشی از آزمایشگاه و کار با عوامل عفونی و سموم،

خطر امنیت زیستی نیز وجود دارد. عوامل بیماری‌های عفونی و سموم ممکن است به سرقت بروند، گم شوند، یا با نیت پلید برای آلوده کردن عمدی همکاران به‌کار روند یا در خرابکاری‌ها و تروریسم بیولوژیک به‌کار روند. (موارد ۱ و ۲ را بنگرید)

طبیعی	اتفاقی	عمدی
شیوع همه‌گیری <b>Epidemics</b> سراسرگیری <b>Pandemics</b>	آلودگی در آزمایشگاه ضعف حفاظتی سهل‌انگاری	خرابکاری بزهکاری بیولوژیک تروریسم بیولوژیک

شکل شماره ۲. طیف خطرهای بیولوژیک و علل آنها



تصویر شماره ۱: تخم اسکاریس

شناسایی خطرهای امنیت زیستی دشوار است زیرا این خطرها بالقوه و در تغییر هستند و مشخص نیستند و به دست فردی ایجاد می‌شوند که در پی دست یافتن به مواد موجود در آزمایشگاه است، یا می‌خواهد در کار آزمایشگاه اختلال ایجاد کند و کسانی را که در آنجا کار می‌کنند به خطر بیاندازد.<sup>[۹]</sup>

اگرچه بسیاری از عوامل بیماری‌های عفونی که مورد مطالعه دانشمندان قرار می‌گیرند به آسانی در طبیعت یافت می‌شوند، اما پاتوژن‌های طبیعی‌ای که قابلیت آسیب‌رسانی به گروهی از انسان‌ها، حیوانات، یا گیاهان را داشته باشند، کمیابند. البته به استثنای مواردی چون شیوع بیماری یا اپیدمی‌هایی که در برخی مناطق رخ می‌دهد. بنابراین افرادی که در پی دستیابی به مواد یا دانش مربوطه هستند، به دنبال آن در مراکزی می‌روند که انواع بسیاری از عوامل بیماری‌های عفونی و سموم با ویژگی‌های معین وجود دارد و از آنها به وفور نگهداری می‌شود.

نمونه برداری‌هایی که از بیماران صورت گرفته است، برای مثال نمونه خون یا بافت نیز یکی دیگر از منابع شناخته شده عوامل بیماری‌های عفونی بالقوه خطرناک است. از این نمونه‌ها در بیمارستان‌ها یا آزمایشگاه‌های تشخیصی نگهداری می‌شود. آزمایشگاه‌های تشخیصی به‌طور معمول موادی را که برای آزمایش دریافت می‌کنند، انبار نمی‌کنند. با این‌همه چنین بخش‌هایی نیز نیازمند بازنگری و افزایش ایمنی روش‌های کار خود برای نابود کردن مواد مصرف‌شده و اطلاعات مربوطه هستند.

پی‌آمدهای سوءاستفاده از عوامل بیماری‌های عفونی و همچنین سموم در درجه نخست بستگی به مشخصات آن و میزان تأثیر آن بر سلامت دارد، اما تأثیرهای اقتصادی و روانی آن نیز شایان توجه جدی است. از همین رو دقت روی عوامل بیماری‌های عفونی خوش‌خیم نیز اهمیت دارد. چنین عواملی اگرچه ممکن است کشنده نباشند، اما قابلیت وارد آوردن خسارت‌های اقتصادی را دارند و می‌توانند آسیب و دردسر ایجاد کنند. نمونه آن در سال ۱۹۸۴ پیش آمد که فرقه را جنیشی Rajneeshee برای مسموم کردن مردم اورگون Oregon ایالات متحده از سالمونلا تیفی عامل بیماری حصبه *Salmonella typhimurium* استفاده کرد.<sup>[۱۰]</sup> بنابراین ضرورت دارد که کار با همه مواد بیولوژیک آلوده‌کننده با رعایت ایمنی و امنیت و کاربرد روش‌های استاندارد صورت گیرد.

**نمونه ۱.** یکی از کارکنان همکارانش را به عمد آلوده می‌کند.

در سال ۱۹۹۶ یک تکنیسین آزمایشگاه مرکز پزشکی سنتپال در دالاس تکزاس، ایالات متحده، شیرینی‌هایی را با باکتری اسهال خونی شیگلا آلوده و باعث بیماری ۱۲ نفر از همکارانش می‌شود. عمدی بودن کار او واضح بود، زیرا او نامه الکترونیکی‌ای برای همکارانش می‌فرستد و می‌نویسد در اتاق قهوه‌خوری شیرینی برای همه هست.

**نمونه ۲.** دانشجویی هم‌خانه‌هایش را به عمد آلوده می‌کند.

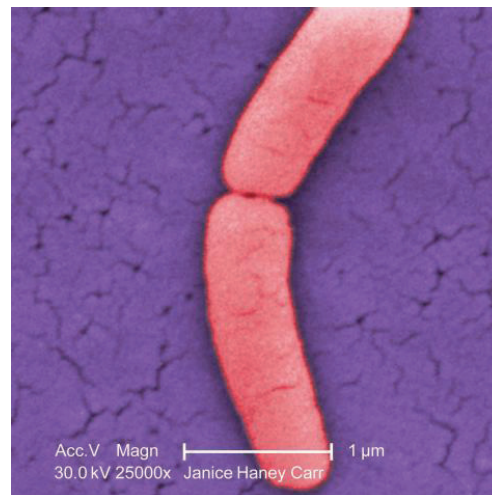
در سال ۱۹۷۲ یک دانشجوی دوره کارشناسی ارشد انگل شناسی دانشگاه مک‌گیل در نزدیکی مونترآل کانادا، خوراک هم‌اتاقی‌های خوابگاهش در مک‌دانلند را با تخم کرم روده *Ascaris suum* آلوده می‌کند. دو تن از چهار هم‌اتاقی دچار نارسایی تنفسی حاد می‌شوند و معاینات نشان می‌دهد که منشأ آن کرم‌های انگلی بوده‌اند. پیش از وقوع این حادثه، دانشجوی یاد شده با هم‌خانه‌هایش مشاجره‌هایی بر سر کرایه آپارتمانی کرده بود که در آن زندگی می‌کردند.

منبع: س. و. کراوس S. W. Craus، «تروریسم بیولوژیک و بزهکاری بیولوژیک: استفاده غیر مجاز از عوامل بیولوژیک از سال ۱۹۹۰»، تز پژوهشی، مرکز پژوهش مبارزه با گسترش سلاحها، دانشگاه دفاع ملی، واشینگتن دیسی، فوریه ۲۰۰۱، صص ۴۳-۴۵، ۶۱



میزان مناسب بودن کاربرد یک عامل بیماری‌های عفونی یا سم در اقدامی با سوءنیت، میزان خطر امنیت زیستی آن را تعیین می‌کند. برآورد این خطرها باید با چنان گستردگی‌ای صورت گیرد که هم بتواند دشمنان بالقوه و توانایی‌های آنان را و هم آسیب‌پذیری‌های سازمان معین را تخمین بزند. برای دنبال کردن یک سناریو (برپایه خطر) می‌توان با شناسایی نقاط ضعف اقدامات امنیت زیستی موجود و پیش‌بینی شده، خطرها را به‌خوبی برآورد کرد. آنگاه می‌توان امکانات موجود را روی اقدامات امنیتی مناسب متمرکز کرد.

مسئولیت برآورد و مدیریت خطرهای امنیت زیستی در درجه نخست بر عهده مدیر سازمان است. مدیران آزمایشگاه و سرپرست‌های پژوهش‌های مختلف می‌توانند در برآورد خطرها کمک کنند، اما یک متصدی زیست ایمنی و امنیت زیستی باید آنان را هماهنگ و هدایت کند. باید صورت موجودی از همه عوامل بیماری‌های عفونی و سم‌های فعال موجود در یک سازمان با هماهنگی مدیریت تهیه شود. در مواردی ممکن است چنین فهرستی از پیش و مطابق با مقررات ایمنی زیستی یا بر پایه تجربه تهیه شده باشد. مدیریت باید کار برآورد خطر را هدایت کند و در مشورت با مجری قانون و کارشناسان امنیتی خطر بالقوه‌ای را شناسایی کند که سازمان را تهدید می‌کند. مدیر آزمایشگاه و پژوهشگر ارشد، دانش و تخصص لازم برای تشخیص عوامل بیماری‌های عفونی و سموم موجود در آزمایشگاه را دارند. در ارزیابی خطر آنان می‌توانند سطح ایمنی زیستی (BSL) موجود را به‌کار گیرند، یا بر اساس طبقه‌بندی گروه خطر عوامل بیولوژیک اقدام کنند.<sup>[۱۱]</sup> برآورد خطر اساس تنظیم برنامه امنیت زیستی «حساب‌شده» برای رسیدگی به مشکلات امنیتی شناخته شده است.<sup>[۱۲]</sup>



تصویر شماره ۲: باکتری Salmonella

### ۲.۳. امنیت زیستی – کاربردی در عمل

اجرای امنیت زیستی بسیاری از جنبه‌های کار و امکانات آزمایشگاه را در برمی‌گیرد و هدف آن تأمین نفوذناپذیری و امنیت همه عوامل بیماری‌های عفونی، سموم و اطلاعات حساس است.

امنیت زیستی – کاربردی چند جزء کلیدی دارد:

- پاسخ‌گویی کارمندان
- کنترل مواد
- ایجاد روش‌های استاندارد کار
- هم‌خوانی با روش‌های امنیت زیستی
- حفاظت فیزیکی
- کنترل دسترسی
- حفاظت اطلاعات
- امنیت حمل‌ونقل
- روال صحیح برای گزارش حوادث امنیتی و نحوه واکنش
- اجرای مداوم ارزیابی و بازرسی
- تمرین و آموزش<sup>[۱۳]</sup>

### ۲.۳.۱. پاسخگویی کارمندان

کارفرما و کارمند در مسئولیت امنیت زیستی شریک هستند، اما مسئولیت پاسخگویی نهایی درباره مواد، دستگاه‌ها، و اطلاعات موجود و کارهای انجام شده در سازمان و اقدامات کارکنان، بر عهده رئیس آن سازمان است. برای یک کارمند دشوار است که اطلاع کامل از همه کارها داشته باشد و بنابراین مسئولیت‌ها اغلب به مدیران آزمایشگاه و سرپرستان پژوهش‌ها سپرده می‌شود. آنان به نوبه خود می‌توانند نظارت بر عوامل معین یا همه عوامل یک آزمایشگاه را به کارمندان دارای صلاحیت لازم بسپارند. این کارمندان باید:

بر عوامل بیماری‌های عفونی، سموم و اطلاعات و دستگاه‌های حساس نظارت و سپس تضمین کنند که حساب همه اینها همیشه نگه داشته می‌شود. باید از آنها صورت‌برداری کنند، حسابرسی کنند و گزارش دهند.<sup>[۱۴]</sup>

شخص یا اشخاص واجد شرایط که مسئولیت دارند، باید بر همه جوانب آنچه قرار است سرپرستی‌اش را کنند، احاطه داشته باشند؛ از لحظه‌ای که آن را تحویل می‌گیرند یا تولید می‌کنند، تا نبودی نهایی یا انتقال آن به بیرون از سازمان. این کارمند یا کارمندان همچنین مسئولیت دارند همه تغییرات در وضع عامل را ثبت کنند و برای مثال در صورت لزوم آن را در فهرست عوامل واگیردار جا دهند. افزون بر آن، کارمند باید ایرادهای موجود در صورت موجودی‌ها را به کارمند ارشد مناسب، مانند مدیر آزمایشگاه، پژوهشگر ارشد، یا متصدی ایمنی و امنیت زیستی گزارش دهد. تقسیم مسئولیت‌ها به کارمندان معین، امکان پاسخگویی کامل هر کارمند برای همه عوامل موجود تحت نظارت یک سرپرست را فراهم می‌کند و کشف سریع مشکلات بالقوه را میسر می‌سازد.

سایر اموال آزمایشگاه که ارزش بالقوه دارند، عبارت هستند از:

- مواد و دستگاه‌ها
- دفترهای یادداشت آزمایشگاه، دفترهای روزانه و اطلاعات خام
- اطلاعات بیماران، صورت موجودی (چه به شکل دیجیتال و چه روی کاغذ)، اطلاعات مربوط به دستگاه‌ها و کارکنان (یعنی جزئیات سازمانی یا امنیتی، صورت اجازه دسترسی افراد به مواد، جزئیات درآمد کارمندان، اطلاعات مربوط به کارکنان، و غیره)
- کامپیوترهای آزمایشگاه
- قبض‌های رسید مواد و دستگاه‌ها.

هر یک از کارمندان یک آزمایشگاه، صرف نظر از نوع استخدام و سطح دسترسی او، به میزان معینی پاسخگویی وظایف خودش است و مسئولیت دارد که امنیت زیستی حفظ شود. این میزان مسئولیت بر پایه صلاحیت‌ها و ارزیابی حرفه‌ای مدیریت، مدیر آزمایشگاه، یا پژوهشگر ارشد به هر کارمندی داده می‌شود.

- ➡ در مورد اطلاعات مربوطه به مواد، دستگاه‌ها و مسئولیت‌هایی که به شما سپرده شده، آگاهی لازم را کسب نمایید.
- ➡ بی‌اندیشید و ببینید آیا در زمینه مسئولیتی که به گردن شما نهاده شده، اعتماد به نفس دارید.
- ➡ خود را به روش‌های استاندارد برای تأمین امنیت زیستی عادت دهید.



### ۲.۳.۲. کنترل مواد

شیوه‌های درست صورت‌برداری، در کنترل مؤثر مواد نقش اساسی دارد و باید عوامل بیماری‌های عفونی و سموم را از هنگامی که به دست سازمان یا آزمایشگاه می‌رسند تا نابودی نهایی یا ارسال آنها، در بر بگیرد.<sup>[۱۵]</sup> شیوه‌های درست صورت‌برداری باید شامل تأیید رسید کالا از سوی مأمور این کار باشد. شیوه‌ها و مقررات درست ایمنی زیستی تا حدودی کنترل موجودی‌ها را نیز مورد بحث قرار می‌دهد، اما این امر عمومیت ندارد.

دسترسی به بخش‌هایی که مواد بیولوژیک در آن استفاده یا نگهداری می‌شود، باید محدود به افرادی با مجوزهای درست باشد. کارمندانی که به مواد بیولوژیک دسترسی دارند و با آنها کار می‌کنند باید وظایف اصلی صورت‌برداری را بر عهده داشته باشند، زیرا آنان با نوع و میزان مواد بیولوژیک موجود و جایگاه و وضعیت آنها آشنایی دارند. قواعد و روش‌های کنترل مواد باید توسط مدیران آزمایشگاه یا سرپرستان پژوهش و با همکاری مدیریت و متصدی ایمنی زیستی و امنیت زیستی تدوین شود. روش‌های موجود زیست ایمنی برای کنترل مواد را می‌توان به عنوان پایه‌ای برای کنترل موجودی‌ها به کار برد، اما این روشها ممکن است با دغدغه‌های امنیتی سازگار نباشند. برای نمونه، فهرست عوامل بیماری‌های عفونی و سموم مورد استفاده در آزمایشگاه را آشکارا بیرون آن نصب می‌کنند تا لزوم احتیاط را گوشزد کنند، اما از دیدگاه امنیت زیستی چنین اطلاعاتی را باید حساس شمرد و نباید آشکارا به همه نشان داده شود. نصب برچسب «خطر بیولوژیک» روی پاکت حاوی اطلاعات مربوط به یک کارمند و فرستادن آن با پست برای تقاضای اطلاعات بیشتر، از مواردی است که ایراد امنیتی دارد.

صورت‌برداری‌های عوامل بیماری‌های عفونی و سموم پیچیدگی‌های گوناگونی دارند، اما لازم است که اطلاعات به جا و مناسبی در آنها گنجانده شود، از قبیل:

- نوع ماده (نام، تیره، گونه سروتایپ، رده‌بندی، و غیره)
- شکل مواد (محللول یا قرص، خشک شده با انجماد یا لیوفیلیزه، پوشیده شده در پارافین و غیره)
- مقدار ماده (تعداد آمپول‌ها، مقدار مایع، مقدار پس از آزمایش)
- جای نگهداری ماده (نگهداری کوتاه‌مدت یا بلندمدت یا هنگام مصرف)
- کارمند رابط یا مسئول
- دستکاری‌های صورت گرفته روی مشخصات بیولوژیک اولیه ماده (یعنی میکروارگانیسم‌هایی که ژن آنها دست‌کاری ژنتیکی شده است)
- گواهی و تاریخ و روش نابودسازی یا غیرفعال کردن ماده
- تاریخ‌های جابه‌جایی ماده (ورود و خروج) و گواهی مصرف‌کننده‌نهایی

برای هدایت و مدیریت صورت‌برداری‌ها روش‌های گوناگونی را می‌توان به کار بست:

- فهرست‌های مواد مختلف را می‌توان در واحدهای آزمایشگاهی و با مدیریت اشخاصی که پاسخگوی آن مواد هستند نوشت و برای کارمندی در مقام بالاتر فرستاد.
- فهرست عمومی برای همه سازمان را می‌توان با هدایت و مدیریت مقام مسئول و متصدی ایمنی زیستی و امنیت زیستی تهیه کرد.
- فهرست عمومی مواد می‌تواند تعداد مواد و میزان دستکاری در آنها را کاهش دهد، یا عوامل بیماری‌های عفونی و سموم واگیردار را با انواع کم خطر آنها جایگزین کند.<sup>[۱۶]</sup>

- چه اطلاعات ویژه‌ای درباره مواد باید ثبت شود، و چه هنگام؟
- اطلاعات مربوط به مواد را چه مدتی باید نگهداری کرد؟
- امنیت اطلاعات مربوط به مواد را چگونه باید حفظ کرد؟
- این اطلاعات در چه فواصل زمانی باید بازنگری و به‌روز شوند؟
- چه کسی باید به اطلاعات مربوط به مواد دسترسی داشته‌باشد؟
- چه کسی و به چه کسی باید ایرادهای صورت‌برداری را گزارش دهد؟

#### ۲.۳.۲.۱. کنترل بیشتر موجودی‌ها

باید دستگاه‌هایی را که کاربردهای دوگانه دارند و مقررات کشوری و بین‌المللی صادرات شامل آنها می‌شود، کنترل کرد. در این مورد نیز باید همان موشکافی و اقدامات امنیتی را اجرا کرد که در مورد صورت‌برداری مواد به کار می‌رود. این اقلام عبارتند از:

- تجهیزات بیوتکنولوژی، شامل همه آزمایشگاه‌های با سطح حفاظت کامل گروه ۳ و ۴ و BSL3 و BSL4
- مخمرها
- سانتریفوژهای جداکننده
- دستگاه‌های فیلتراسیون
- دستگاه‌های لیوفیلیزاتور
- اتاقک‌های بیوآئروسول
- دستگاه‌های اسپری و مه‌ساز<sup>[۱۷]</sup>

#### ۲.۳.۳. حفاظت فیزیکی

هدف از حفاظت فیزیکی عبارت است از محدود کردن دسترسی به مواد به افراد دارای صلاحیت حرفه‌ای و کسانی که مصونیت‌های لازم را برای کار با عوامل بیماری‌های عفونی معین دارند و ایجاد تأخیر، ممانعت و کشف دسترسی افراد غیر مجاز به مواد. حفاظت فیزیکی بستگی نزدیکی با ایمنی زیستی و طراحی محل دارد. با این همه، حتی پیچیده‌ترین حفاظت فیزیکی خود تنها جزئی از یک محل کار امن است. سطح امنیت آزمایشگاه یا محل در نهایت از میزان آگاهی کارمند به لزوم امنیت و از رفتار او که این آگاهی را نشان می‌دهد، مشخص می‌شود.

حفاظت فیزیکی موارد زیر را در برمی‌گیرد:

- مراقبت و مدیریت محیط پیرامون و مرزهای امنیت
- ایجاد محدودیت دسترسی
- نصب و نگهداری دستگاه‌های آژیر و مراقبت
- تعیین و حفظ سطوح مناسب حفاظت
- تأمین امکان اعلام خطر فوری در موارد نقض امنیت یا نفوذ غیر مجاز

امروزه دستگاه‌های گوناگونی برای محدود کردن دسترسی افراد به اطلاعات سازمان‌ها به منظور کشف هرگونه دسترسی غیر مجاز (نفوذ) استفاده می‌شود. پیچیدگی این دستگاه‌ها متناسب با آنچه



حفظ امنیت سازمان ایجاب می‌کند، بالا می‌رود. جدول شماره یک فهرستی از اجزای حفاظت فیزیکی را نشان می‌دهد که برای محدود کردن دسترسی و تأمین مراقبت از امکانات آزمایشگاه‌ها می‌توان به کار برد.

سطح ایمنی زیستی (BSL) تعیین شده در یک محل یا آزمایشگاه، سطح حفاظت لازم برای کار ایمن را تعیین می‌کند. (جدول شماره ۲)<sup>[۱۸]</sup> سطح خطر امنیت زیستی متناسب است با درجه BSL. هرچه این درجه بالاتر باشد، حفاظت فیزیکی نیز باید بالاتر باشد. با بالاتر رفتن سطح خطر، لازم است که سطح محدودیت دسترسی و پیچیدگی دستگاه‌های مراقبت نیز بالا رود.

در اغلب موارد دسترسی به بخش‌های مشمول «حفاظت کلی» برای همه کارمندان مجاز آزاد

است و تنها محدود به دیوارهای ساختمان

است. میهمانان و بازدیدکنندگان را نیز پس

از بازرسی و پس از نصب کارت شناسایی

روی سینه می‌توان به ساختمان راه داد. ورود

افراد را می‌توان با درهای قفل شده‌ای که با

کلید سنتی، کلید رمزی، و یا با کارت‌های

الکترونیکی باز می‌شوند کنترل و یا در را

توسط نگهبانی که کارت شناسایی را تأیید

می‌کند باز کرد.

بخش‌های «ممنوعه» عبارتند از آزمایشگاه‌های BSL1 و BSL2 برای کارهای میکروبیولوژی با

محدودیت پایین تا متوسط. فقط کارمندانی که اجازه ورود به بخش‌های ممنوعه را کسب کرده‌اند

باید حق ورود به آنجا را داشته

باشند. بسیاری از آزمایشگاه‌ها

در همین سطح از طبقه‌بندی جا

می‌گیرند. این آزمایشگاه‌ها خطر

ناچیزی برای انسان‌ها دارند و کار

آنها فقط گیاهان و حیوانات را در

برمی‌گیرد.

بخش‌های «ورود مطلقاً ممنوع» لایه‌های امنیتی بیشتری دارند تا از عوامل عفونی و سموم با خطر

متوسط به بالا در آزمایشگاه‌های BSL3 و BSL4 حفاظت کنند. در این آزمایشگاه‌ها بالاترین سطح

حفاظت و محدودیت برقرار است.

جدول شماره ۱. اجزای حفاظت فیزیکی برای کنترل دسترسی و مراقبت

کنترل دسترسی	مراقبت
• محیط آزمایشگاه یا واحد (از قبیل نرده‌ها، دیوارها)	• تلویزیون‌های مدار بسته
• قفل‌ها، دگمه‌های قفل رمزی، دستگاه‌های خوانش کارت الکترونیکی	• دوربین‌های دید در تاریکی و مادون قرمز
• اسکانرهای مشخصات بیومتریک	• دتکتورهای حرکت (از قبیل مادون قرمز غیر فعال، حسگرهای ریزموجی یا ماورای صوتی)
• کارت‌های شناسایی در معرض دید	• دستگاه‌های ضبط صدا
• نگهبان	• نگهبان
• طراحی محل	

جدول شماره ۲. سطوح ایمنی زیستی و سطوح مربوطه در خطر امنیت زیستی و حفاظت فیزیکی

سطح حفاظت	سطح خطر زیست‌امنیتی	سطح حفاظت فیزیکی
موردی ندارد	ناچیز یا پایین	حفاظت کلی
BSL1 و BSL2	پایین تا متوسط	ممنوع
BSL3	متوسط تا بالا	مطلقاً ممنوع
BSL4	بالا	مطلقاً ممنوع

بخش‌های مشمول رعایت امنیت را شناسایی کنید و هنگام حضور در این بخش‌ها و با دستگاه‌های مشمول محدودیت، نگرشی حرفه‌ای نسبت به امنیت داشته باشید.

تنها به موانع فیزیکی برای ایجاد امنیت اعتماد کنید. (رفتار انسان مهم‌ترین جزء از سیستم امنیتی است).

سهل‌انگاری در رعایت امنیت را بی‌درنگ به شخص بی‌دقت یا مقام مافوق گزارش دهید.



## ۲.۳.۳.۱. کنترل دسترسی

محدود کردن دسترسی به امکانات و آزمایشگاه‌ها هم جزئی از ایمنی زیستی و هم جزئی از امنیت زیستی است. مدیریت و کارمندانی که اجازه دسترسی به بخش‌های ممنوعه را صادر می‌کنند مسئولیت دارند تا کسب اطمینان کنند که افراد دارای مجوز ورود به این بخش‌ها صلاحیت لازم را برای این کار دارند و یا آموزش کامل روش‌های کار و رفتار در آزمایشگاه را پشت سر گذاشته‌اند. بسیاری از آزمایشگاه‌ها کارمندی را برای مراقبت و صدور اجازه ورود به بخش‌های معین، از قبیل اتاق‌های حفاظت شده، استخدام می‌کنند.

اگر محدودیتی در دسترسی کارمندان فاقد صلاحیت یا فاقد ایمنی به امکانات و آزمایشگاه‌ها نباشد، ابتلای اتفاقی یا آسیب‌های دیگر می‌تواند روش جاری ایمنی زیستی را نقض کند و به تخطی از قوانین کشور در زمینه محیط کار و بهداشت کار بیانجامد. میزان مجاز دسترسی به آزمایشگاه‌ها بستگی به کار انجام شده و مواد مصرف شده دارد. هرچند که تقسیم فضای کار بستگی به امکانات موجود دارد، اما ایمنی زیستی و امنیت زیستی را نیز باید در نظر گرفت.

صدور اجازه ورود به بخش‌های نگهداری از پاتوژن‌های پر خطر باید بر مبنای صلاحیت‌های حرفه‌ای صورت بگیرد. ممکن است مدیریت بخواهد شیوه‌های دست‌چین کردن دیگری را هم به کار ببرد، از قبیل بررسی سوابق کارمند. درواقع برای تأیید یک کارمند ممکن است بررسی سوابق یا معیارهای دیگری نیز مطرح شود.

دسترسی به بخش‌های ممنوعه را باید در فواصل زمانی معین مورد بررسی مجدد قرار داد تا به این شکل بتوان ممنوعیت‌های بی‌مورد را برطرف کرد یا در صورت مشاهده سهل‌انگاری، اجازه‌ای را باطل کرد.

در مواردی که ورود به یک محل یا بخش ممنوعه بدون حضور سرپرست صورت می‌گیرد، کارمندی که به آنجا رفت و آمد می‌کند باید خطر لو رفتن اطلاعات لازم برای ورود را به حداقل برساند. برای مثال هنگام فشردن دکمه‌های رمز ورودی، از دور می‌توان دکمه‌ها را خواند و کارت‌های کلید مغناطیسی را به آسانی کپی کرد، اما اگر این دو با هم به کار روند سطح امنیت بالاتر می‌رود. زیرا کارت یا رمز به تنهایی نمی‌تواند راه ورود را باز کند. برای بالا بردن میزان امنیت بهتر است رمزهای ورودی هر از چندگاه عوض شوند. با این‌همه در پوشیده نگاه داشتن رمز ورودی از دید دیگران و حفاظت از کلیدهای کارت، کارمندان نقش اصلی را دارند.

کارمندان باید روش‌های امنیتی را به هنگام استفاده از درهای ساختمان یا بخش‌های امن به خوبی به کار بگیرند. درها هنگام بسته شدن باید به شکل خودکار قفل شوند و طول مدت باز بودن آنها باید حداقل باشد تا فرصتی به ورود افراد غیر مجاز (معروف به ورود سایه به سایه *tailgating*) داده نشود. نباید گذاشت یک شخص غیرمجاز با دنبال کردن یک کارمند مجاز، وارد محل ممنوعه شود. شخص غیر مجاز می‌تواند برگ‌های جعلی حاکی از جا گذاشتن یا گم کردن کلید کارت یا کلید معمولی نشان دهد، یا بهانه‌های دیگری بترشد مبنی بر این که به تنهایی وارد نمی‌شود. اگر با او بحث کنید، این شخص ممکن است شروع کند به دلیل تراشی یا شاید پرخاش کردن، اما نکته حیاتی این است که برای دیدن نشانه شناسایی درست باید اصرار کرد. در صورت نیاز باید از همکاران یا مأموران امنیتی کمک خواست.



کارمندان باید هنگام پایان استخدامشان کلیدها را تحویل دهند. گزارش فوری گمشدن کلیدها و کلیدهای کارتی نیز اهمیت دارد. کلیدها و کلیدهای کارتی مشابه را باید نابود کرد و از مجموعه تازهای استفاده کرد.

- هنگام فشردن دکمه‌های رمز ورودی به ساختمان یا بخش ممنوعه هشیار باشید.
- هرگز درباره رمزهای ورودی با کسی صحبت نکنید.
- از نوشتن رمز ورودی یا ثبت الکترونیکی آنها پرهیز کنید.
- از کسی که خود به تنهایی نمی‌تواند وارد جایی شود نشانه شناسایی بخواهید. اگر شخص نمی‌تواند نشانه شناسایی ارائه کند، بیدرنگ این موضوع را به رئیس حفاظت گزارش دهید یا خود اقدام لازم را انجام دهید.
- کلیدهای کارتی مصرف نشده را پس بفرستید و گم شدن آنها را بیدرنگ گزارش دهید.
- قفل کردن درها، شامل دفترهای کار و انبارها را به روش جاری تبدیل کنید.

#### ۲.۳.۴. حفاظت اطلاعات

اطلاعات لازم برای دسترسی به امکانات یا مواد بیولوژیک، اطلاعات حساسی هستند و باید از آنها حفاظت کرد.<sup>[۱۹]</sup> اقدامات حفاظتی برای اطلاعات حساس دیگری نیز ممکن است لازم باشد، از قبیل:

- صورت موجودی عوامل عفونی و سموم
- دستگاه‌های حساس و محل قرارگیری آنها
- روال حفاظت
- لیست ورود و خروج
- اطلاعات نمونه‌های مربوط به بیماران
- اطلاعات تماس با کارمندان<sup>[۲۰]</sup>

اطلاعات حساس را باید به شکل الکترونیک و در کامپیوترهای بیرون از شبکه و همچنین چاپ شده روی کاغذ در قفسه‌های قفل شده نگهداری کرد. اطلاعات را هرگز نباید در وسایل ذخیره‌سازی از قبیل حافظه‌های USB جابه جا کرد. به منظور کسب اطمینان از این که اطلاعات موجود صحت دارد و اطلاعات کهنه از دسترس خارج شده است، کپی‌های قدیمی را باید نابود کرد.

دیوارهای آتش **firewall** سخت افزاری (فیزیکی) قابل اعتمادتر از برنامه‌های نرم‌افزاری هستند و اغلب در سازمان‌های بزرگ به کار می‌روند. لازمه کاربرد برنامه‌های نرم‌افزاری ضد ویروس، به روز کردن مرتب پرونده تشخیص ویروس آنها است. به روز نگاه داشتن سیستم عامل کامپیوتر نیز به همان اندازه مهم است. کامپیوترهای خانگی بعید است که حفاظت کافی داشته باشند و از نگهداری اطلاعات حساس در آنها باید پرهیز کرد.

اطلاعات موجود در لوح سخت کامپیوترها را هم می‌توان بازسازی کرد، حتی اگر آن را پاک کرده باشند یا فورمت کرده باشند. یکی از راه‌های جلوگیری از بازسازی اطلاعات استفاده از نرم‌افزارهای رمزنویسی است. اینگونه نرم‌افزارها به آسانی و به شکل رایگان **freeware** در دسترس هستند. نرم‌افزار رمزنویسی را به هنگام انتقال اطلاعات حساس با ایمیل نیز باید به کار برد. به هنگام دور انداختن کامپیوترهای کهنه نیز باید مواظب بود که اطلاعات حساس در آنها باقی نمانده باشد و از همین رو لوح سخت آنها را باید برداشت. بسیاری از سازمان‌ها بخش مستقل یا مشترک فن‌آوری اطلاعات (IT) دارند.

در موارد زیر باید با بخش فناوری اطلاعات مشورت کرد و راهنمایی گرفت:

### ۲.۳.۵. امنیت جابه‌جایی و حمل و نقل

جابه‌جایی عوامل عفونی و سموم خطرناک باید از راهبردهای کشوری و جهانی که بر پایه

- شناسایی اطلاعات حساس و مقرر روشن برای حفظ ایمنی و امنیت آن‌ها.
- استفاده از ابزارهای موجود حفاظت فناوری اطلاعاتی برای تأمین نفوذناپذیر بودن اطلاعات.
- پرهیز از نگهداری اطلاعات حساس در کامپیوترهای خانگی.
- پرهیز از جابه‌جایی اطلاعات حساس از طریق ای‌میل.
- به‌روز نگاه‌داشتن اطلاعات حساس و نابودی اطلاعات (شامل سی‌دی‌ها و دی‌وی‌دی‌ها).
- انتخاب رمزهای ورود پیچیده که مجموعه‌ای از حروف بزرگ و ارقام گوناگون باشد.
- تعویض مرتب رمز ورود.

آیین‌نامه‌های سازمان ملل متحد برای دو دسته از پر خطرترین مواد (دسته الف و ب) بنا شده است، پیروی کند.<sup>[۲۱]</sup> آیین‌نامه‌های سازمان ملل بر ایمنی کارمندی که در حمل و نقل مواد نقش دارند و بر خدشه‌ناپذیر بودن حفاظت تأکید دارد (مطالعات موردی شماره ۳ تا ۶ را به عنوان نمونه‌هایی از نقض

**نمونه ۳.** باسیل زنده سیاه زخم *Bacillus anthracis* به اشتباه ارسال شد.

در ماه مه ۲۰۰۴ باسیل زنده سیاه زخم از مؤسسه پژوهشی سائوترن در شهر فردریک ایالت مریلند ایالات متحده آمریکا به بیمارستان کودکان و مرکز تحقیقات اوکلند در شهر اوکلند کالیفرنیا ایالات متحده آمریکا ارسال شد. ارسال‌کننده گواهی کرده بود که نمونه‌های ارسالی زنده نیستند. با این همه مرگ ۴۹ موش که با استفاده از نمونه‌های آن باسیل سیاه‌زخم آلوده شده بودند نشان داد که آنها زنده بودند.

منبع: روسلی R. Vesely، «حادثه سیاه‌زخم شایان توجه است»، روزنامه Oakland Tribune، ۱۲ ژوئن ۲۰۰۴

**نمونه ۴.** روزنامه‌نگاران انگلیسی یک رشته از دی‌ان‌ای DNA دستکاری شده آبله را سفارش دادند. در چهاردهم ژوئن ۲۰۰۶ روزنامه گاردین گزارش داد که روزنامه‌نگاران موفق شده‌اند از طریق اینترنت یک آمپول پلاستیکی حاوی رشته‌ای به طول ۷۸ جفت باز از دی‌ان‌ای پروتئین پوسته ویروس آبله را که با دستکاری سه جهش در آن ایجاد شده بود، از شرکت ویاج بایو لی میتد VH Bio Ltd سفارش دهند و آنها را دریافت کنند. قیمت این آمپول که در پاکت ضخیم دریافت شد، ۳۳ پوند بود. شرکت فروشنده نمی‌دانست که آن رشته متعلق به ژنوم آبله است.

منبع: ج. راندرسون J. Randerson، «افشاگری: قوانین سهل‌انگاران‌های که ساخت دی‌ان‌ای ویروس مرگ‌زا را مجاز می‌کنند»، گاردین، ۱۴ ژوئن ۲۰۰۶

**نمونه ۵.** تقاضای باسیل سیاه‌زخم از دانشگاه گوتنبرگ سوئد

دانشگاه گوتنبرگ سوئد که یکی از بزرگترین ذخایر باکتری‌های جهان را دارد، از هنگام ارسال نامه‌های آلوده به سیاه‌زخم در ایالات متحده در سال ۲۰۰۱، دو مورد تقاضای ارسال باسیل سیاه‌زخم دریافت کرد که مشکوک تشخیص داده شدند. این تقاضاها برای بررسی به پلیس امنیتی سوئد تحویل داده شدند. دانشگاه گوتنبرگ اعلام کرد که در ذخایر آن هرگز باسیل سیاه‌زخم نگهداری نشده و به کسی ارائه نشده است.

منبع: اکو، رادیوی سوئد، ۱۷ مه ۲۰۰۶

**نمونه ۶.** باسیل طاعون *Yersinia pestis* به تانزانیا ارسال شد.

در سپتامبر ۲۰۰۲ توماس باتلر، پروفیسور دانشگاه صنعتی تگزاس در شهر لوبوک ایالت تگزاس در ایالات متحده آمریکا، عامل طاعون (طاعون خیارکی، bubonic plague) را دانسته و بدون کسب مجوز لازم از وزارت بازرگانی ایالات متحده به تانزانیا انتقال داد. او در بازنامه این عامل عفونی را «مواد آزمایشگاهی» قلمداد کرد و از پر کردن بخش‌های مربوطه در اظهارنامه الزامی طرف صادرکننده سر باز زد. از این‌رو باتلر متهم شد که مفاد مقررات اداره صادرات ایالات متحده را به عمد زیر پا گذاشته است. در دهم مارس ۲۰۰۴ باتلر به دوسال زندان و سه سال حبس تعلیقی محکوم شد. او همچنین برای زیر پا نهادن قوانین صادرات و اظهارنامه جعلی به پرداخت جریمه جزایی و پرداخت غرامت محکوم شد.

منبع: م. انسرینک و د. ملکوف M. Enserink & D. Malakov، «محاکمات توماس باتلر»، ساینس، جلد ۳۰۲، شماره ۵۶۵۳ (۱۹ دسامبر ۲۰۰۳)، صص ۲۰۵۴-۶۳.



روش‌های درست یا اشتباه در کار ملاحظه کنید). برای حمل و نقل در فواصل کوتاه، مانند میان دو محل هم‌جوار یا در داخل یک محل نیز باید اقدامات حفاظتی کافی به عمل آید. هنگام انتقال مواد در داخل یک محل یا میان دو محل، موادی که درست بسته‌بندی شده‌اند نباید حتی یک لحظه از دیدرس دور شوند. به این شکل خدشه‌ناپذیر بودن جابه‌جایی در تمام طول راه تا رسیدن به مقصد تأمین می‌شود.<sup>[۲۲]</sup> برای حمل و نقل‌های طولانی‌تر باید از امکانات حرفه‌ای استفاده کرد و شرکت‌های بسیاری هستند که در انتقال محموله‌های خطرناک کار می‌کنند و گواهینامه آدی‌آر (ADR حمل و نقل ایمن و بین‌المللی محموله‌های خطرناک در جاده‌ها) را دارند.<sup>[۲۳]</sup> نخستین مسئله جابه‌جایی در مسافت‌های طولانی آن است که فرستنده خود نمی‌تواند به شخصه کار جابه‌جایی را سرپرستی کند و باید به شرکتی که کار را گرفته است اعتماد کند. در این موارد فرستنده باید زنجیره‌ای از مراقبت‌ها را ایجاد کند تا بتواند:

- افراد درگیر در جابه‌جایی را شناسایی کند.
- اقداماتی را برای هنگام بروز خطرهای احتمالی پیش‌بینی کند.

مدیریت یا متصدی زیست ایمنی و امنیت زیستی باید در جریان جابه‌جایی مواد پرخطر قرار بگیرند. متصدی ایمنی زیستی و امنیت زیستی می‌تواند در سازماندهی بسته‌بندی ایمن و انتخاب حامل مناسب برای جابه‌جایی امن مواد کمک کند. هر قدر هم که عوامل عفونی یا سم خوش‌خیم باشد، برای کسب اطمینان در حمل و نقل ایمن و امن آنها، چند شرط باید برآورده شود:

- گیرنده باید شناخته‌شده و مورد اعتماد باشد. اگر این شناخت وجود ندارد، باید ارتباط او با مؤسسات پژوهشی یا با شرکت‌های تجاری از طریق اینترنت بررسی شود و جستجوی شایستگی‌های علمی او با PubMed صورت گیرد تا صلاحیت حرفه‌ای گیرنده مورد تأیید قرار بگیرد.<sup>[۲۴]</sup>
- شرکت حمل و نقلی که کار جابه‌جا کردن مواد را برعهده می‌گیرد باید گواهینامه معتبر کار با محمولات خطرناک را داشته باشد. خط مشی این شرکت در مورد محموله‌های گمشده یا به سرقت رفته باید معلوم باشد و اگر محموله‌ای گم شد یا به سرقت رفت باید بتواند توصیه‌های لازم را بکند. واکنشی که لازم است عبارت است از اطلاع دادن به مراجع قانونی و همچنین به فرستنده و گیرنده.
- فرستنده باید مطمئن باشد که ماده مورد نظرش درست ارسال و درست بسته‌بندی می‌شود.
- به‌هنگام تحویل، گیرنده باید رسیدی را امضا و تأیید کند که ماده رسیده است و با مشخصات ماده سفارش داده شده مطابقت دارد. گیرنده باید رسید را با پست یا با فکس برای فرستنده ارسال کند. آنگاه فرستنده دیگر مسئولیتی در قبال ماده ارسال شده ندارد. همه اطلاعات باید مستند شوند و امکان ردیابی ماده ارسالی وجود داشته باشد.<sup>[۲۵]</sup>

بسیاری از کشورها در تلاش برای منع گسترش سلاح‌های کشتار جمعی و از آن‌جمله سلاح‌های بیولوژیک، قوانینی برای صادرات مواد، دستگاه‌ها و فناوری بیولوژیک دارند. مطابق آییننامه شماره ۳۳۸۱/۹۴/EEC شورای اتحادیه اروپا، کشورهای عضو اتحادیه اروپا از صادرات بدون مجوز اقلامی که فهرست آنها در پیوست آیین‌نامه آمده منع شده‌اند.<sup>[۲۶]</sup> اقلام موجود در فهرست پیوست از جمله شامل عوامل عفونی و سموم خطرناک برای انسان، حیوانات و گیاهان است.

در واکنش به مصوبات شورای امنیت سازمان ملل متحد، بسیاری کشورها در مبارزه با تروریسمی که در جبهه‌های تازه‌ای، از جمله با استفاده از مواد بیولوژیک حمله می‌کند، قوانینی وضع کرده‌اند. هنگام پیاده کردن قوانین در سطح کشوری، صادرات بدون مجوز اقلام فهرست شده، غیرقانونی به شمار می‌رود.<sup>[۲۷]</sup> اگر صادرکننده محکوم شود، سازمان یا کارمند مربوطه ممکن است کیفرهای جزایی یا اداری ببینند یا جریمه شوند. بنابراین، فرستنده باید سیستمی ایجاد کند تا بتواند تشخیص دهد که ارسال مواد با قوانین صادرات موجود مطابقت دارد و پیمان‌ها و تحریم‌های مربوطه را نقض نمی‌کند. مراجع نظارت بر صادرات اغلب جلسات علنی برای توضیح قوانین جاری صادرات برگزار می‌کنند. مقامات کشوری همچنین اغلب خواهان بازدید از سازمانها هستند تا اطلاعاتی در مورد قوانین نظارت بر صادرات ارائه دهند.

- برای جابه‌جایی و انتقال مواد، همواره با مدیر آزمایشگاه یا پژوهشگر ارشد مشورت کنید و از وضعیت درست نمونه‌ها کسب اطمینان کنید.
- هنگام ارسال عوامل بیماری‌های عفونی و سموم، از طریق واریسی گواهینامه‌ها و وابستگی‌های گیرنده، مجاز بودن او را بررسی کنید.
- هرگز چیزی را برای گیرنده ناشناس نفرستید.
- لازم است یک زنجیره مراقبت، هنگام حمل و نقل مواد ایجاد کنید.
- در طول جابه‌جایی مواد بیولوژیک پر خطر و در مراکزی که سطح امنیت زیستی پایین است، هرگز این مواد را بی‌مراقبت رها نکنید.
- همواره از کارکنان صلاحیت‌دار و آموزش‌دیده استفاده کنید و روش‌های درست به کار ببندید. از جمله رسیدن نهایی به هنگام تحویل مواد را دریافت کنید.

علاوه بر این‌ها به نکات زیر نیز توجه کنید:

- قوانین ناظر بر صادرات کشورتان را بیاموزید و رعایت کنید (تعریف صادرات در قانون چیست؟ آیا شما صادرکننده شمرده می‌شوید؟)
- مطمئن شوید جابه‌جایی‌هایی که در انتظار نوبت هستند، با قوانین ملی و بین‌المللی صادرات مطابقت دارند.
- پیرامون اینکه چه فرصت‌هایی برای بحث پیرامون نظارت بر صادرات با مقامات کشورتان در پیش‌رواست، اطلاعات بیشتری کسب کنید.
- از شرکت حمل و نقل بپرسید: آیا روش‌هایی برای تأمین امنیت حمل محموله‌های خطرناک دارند؟



### ۳- سرپرستی امنیت زیستی کاربردی

#### ۳.۱. نکات مورد توجه مدیر آزمایشگاه و پژوهشگر ارشد در امور امنیت زیستی

تضمین ایمنی و امنیت در نگهداری و کار با عوامل بیماری‌زا و سموم، لازمه هرگونه فعالیت علوم زیستی برای جلب اعتماد مردم و مقامات تصمیم‌گیرنده است. این حراست همچنین تعهدی جهانی مندرج در کنوانسیون سلاح‌های بیولوژیک و سمی است که پس از تنظیم آن در ۲۶ مارس ۱۹۷۵ بالغ بر ۱۶۳ دولت آن را تصویب و امضا کرده‌اند.<sup>[۲۸]</sup> قطعنامه شماره ۱۵۴۰ شورای امنیت سازمان ملل متحد ایجاب می‌کند که دولت‌های عضو سازمان ملل قوانینی به تصویب برسانند و اقدامات لازم دیگری به عمل آورند تا سلاح‌های بیولوژیک را ممنوع و از گسترش آنها پیشگیری کنند. این قطعنامه دولت‌ها را ملزم می‌سازد که نظارت بر مواد مربوطی را که می‌توانند برای ساختن چنین سلاح‌هایی به کار بروند تأمین و تضمین کنند.<sup>[۲۹]</sup>

میزان هشیاری امنیتی و ادراک خطر از دانشمندی تا دانشمند دیگر و از کشوری تا کشوری دیگر بسیار متفاوت است. افزون بر آن جامعه دانشمندان در پذیرش خطرهای نظری از قبیل خرابکاری داخلی و تروریسم بیولوژیک تا حدودی بی‌میل است. برای نمونه ایالات متحده آمریکا بر پژوهش «دفاع بیولوژیک» و اجرای مقررات کشوری در کارها و سازمان‌های علوم زیستی تأکید بیشتری کرده و این خود مشکلات تازه‌ای از جمله در زمینه جابه‌جایی مواد و دانش مربوطه ایجاد کرده است.<sup>[۳۰]</sup> باید توازنی پیدا کرد: عمل به تعهدهای بین‌المللی برای ایجاد امنیت عوامل بیماری‌های عفونی و سموم، دستگاه‌ها، فناوری و اطلاعات حساس و پیشگیری از افتادن آنها به دست افراد ناباب یا سوءاستفاده از آنها، باید بدون ایجاد مزاحمت برای جامعه علمی صورت بگیرد. امنیت زیستی کاربردی رویکردی را ایجاب می‌کند که هم متوازن است و هم انعطاف‌پذیر و هم با جدیت خطرهای نظری را در ترکیب با این آگاهی مورد بحث قرار می‌دهد که خطرهای امنیتی پیوسته در تغییر هستند.

#### ۳.۲. مدیریت امنیت زیستی کاربردی

یک برآورد جامع از خطرهای امنیت زیستی در چهارچوب این کتابچه راهنما نمی‌گنجد و قانون‌گذاری لازم است تا همه سازمانها و آزمایشگاه‌ها را به اجرای این برآورد ملزم کند. با این همه مدیران آزمایشگاه‌ها و سرپرستان پژوهش‌ها وظیفه دارند که ایمنی زیستی و امنیت زیستی را در آزمایشگاه‌ها بهبود بخشند و از اموال زیر سرپرستی خود حراست کنند. خطرهای امنیت زیستی و شیوه مدیریت آنها را با اجرای سناریوهای برآورد خطر و با تهیه فهرست خطرناک‌ترین عوامل می‌توان به بهترین نحو شناسایی کرد. سیستم استاندارد طبقه‌بندی میزان ایمنی زیستی را می‌توان برای این شناسایی به کار برد.

### ۳.۲.۱. مدیریت مواد

#### ۳.۲.۱.۱. کنترل موجودی‌ها

«کنترل موجودی‌ها» را می‌توان خلاصه کرد در داشتن نظارت کامل بر همه مواد عفونی و سموم موجود در حوزه حفاظتی. اجرای درست کنترل موجودی‌ها این فایده را دارد که پاسخگویی کامل و مداوم تضمین می‌شود (بنگرید به بخش ۲.۳.۲). فقدان صورت‌برداری دقیق خود یک خطر امنیتی است و همچنین تهدیدی برای ایمنی کارمندان آزمایشگاه است. در بسیاری از آزمایشگاه‌ها اجازه داده می‌شود که نمونه‌ها را ذخیره کنند و به این شکل خطری بالقوه ایجاد می‌شود. کنترل درست موجودی‌ها همچنین کشف سریع ناهم‌خوانی‌ها را امکان‌پذیر می‌سازد که این خود در زمینه امنیت اهمیت بزرگی دارد. به‌علاوه، اگر معلوم شود که سازمان یا آزمایشگاهی منشأ عوامل عفونی است و از اطلاعات آن سوءاستفاده شده است، صورت موجودی‌ها را برای دفاع از شیوه کار آن آزمایشگاه می‌توان به‌کار برد.

#### ۳.۲.۱.۲ - اطلاعات موجودی‌ها

باید معین کرد چه اطلاعاتی در صورت موجودی‌ها گنجانده شود. تغییر مقدار مواد به هنگام آزمایش‌ها نیز باید منعکس شود. مشخصات پیشنهادی صورت‌برداری مواد در بالا مورد بحث قرار گرفت (بخش ۲.۳.۲ را بنگرید). صورت موجودی‌ها به دلیل درج اطلاعات حساس می‌بایست حساس شمرده شوند و همچنین توسط کارمند مسئول این کار و با رعایت جوانب امنیت، استفاده و نگهداری شوند.

#### ۳.۲.۱.۳ - مواد مصرفی

نشان دادن و ثبت پارامترهای آزمایش شیوه خوبی در کار آزمایشگاه است و اطلاعات ارزشمندی برای به‌روز کردن صورت موجودی‌ها به دست می‌دهد. تعیین مقدار مواد در حال مصرف شاید دشوار باشد، به‌ویژه به هنگام کشت دادن یا عملیات دیگری که طی آنها تعداد نمونه‌ها و حجم آنها در دوره‌های کوتاه زمانی با مقدار قبلی آنها مطابقت ندارد. در طول استفاده آزمایشی باید به نمونه‌ها شناسه یا شماره نمونه تازه‌ای داد و بار دیگر در صورت موجودی‌ها وارد کرد. نابود کردن مواد نیز باید ثبت شود.

#### ۳.۲.۱.۴ - مواد نگهداری شده

صرف‌نظر از این که مواد به مدت کوتاه یا بلند نگهداری می‌شوند، نگهداری آنها باید با رعایت مقررات حفاظتی باشد و با طبقه‌بندی مناسب ایمنی زیستی و بندهای دستورالعمل‌های جاری ایمنی زیستی مطابقت داشته باشد. مواد زیستی سطح BSL4 باید تمام مدت در آزمایشگاه‌های حفاظتی BSL4 نگهداری شوند و صورت‌برداری دقیق این قبیل مواد باید برقرار باشد تا آنکه مواد زیستی به تمامی غیر فعال و ایمن شناخته شوند. آنگاه می‌توان آنها را از بخش حفاظتی BSL4 به بیرون انتقال داد.<sup>[۳۱]</sup> همچنین مواد زیستی سطح BSL3 باید در شرایط مشابهی در آزمایشگاه حفاظتی BSL3 نگهداری شوند، اما ممکن است این کار به دلیل کمبود جا میسر نباشد. نقض روال درست هم در زمینه ایمنی زیستی و هم در زمینه امنیت زیستی باید مورد توجه قرار گیرد. کارهای BSL را باید



منطبق با ظرفیت موجود امکانات حفاظتی پذیرفت، نه آن که روش‌های درست را به علت کمبود جا تغییر داد.

### ۳.۲.۱.۵ - دریافتی‌های تازه

دریافتی‌های تازه باید بی‌درنگ در سیستم موجودی‌ها گنجانده شوند تا بتوان با این سیستم اداره‌شان کرد. برای وارد کردن یک عامل عفونی یا سم دستکاری شده در صورت موجودی‌ها ممکن است کسب اجازه از مقامات کشوری یا اطلاع دادن به آنان لازم باشد. سازمان مربوطه ممکن است ناگزیر شود تضمین کند که با استفاده از رهنمودهای حفاظتی مناسب BSL امکان نگهداری و کار ایمن با مواد تازه را دارد و برآورد کامل خطرهای ایمنی زیستی به عمل آمده است. سرپرست واجد شرایط باید معین کند کدام کارمندان اجازه دسترسی به مواد تازه را دارند و این تصمیم باید به دیگر کارمندان نیز اطلاع داده شود.

### ۳.۲.۱.۶ - دستگاه‌های آزمایشگاهی حساس

بخشی از دستگاه‌های آزمایشگاه که تحت نظارت قوانین و مقررات صادرات بین‌المللی هستند ممکن است "حساس" تلقی شوند. این قبیل دستگاه‌ها می‌توانند مورد علاقه دشمن باشند. گروه استرالیا مجموعه‌ای غیر رسمی از ۴۱ کشور است که بر اقداماتی پیرامون صدور مجوز صادرات برخی مواد شیمیایی، عوامل بیولوژیک و دستگاه‌های مربوطه تأکید دارد و هدف آن مبارزه با گسترش عوامل شیمیایی و بیولوژیک است.<sup>[۳۲]</sup> فهرستی از عوامل عفونی، سموم و دستگاه‌های برگزیده‌ای که نیازمند کسب مجوز صادرات است در تارنمای این گروه منتشر شده است (همچنین بنگرید به بخش ۲.۳.۲.۱). دستگاه‌های مشمول این رده‌بندی را باید در امنیت نگهداری کرد و بتوان هر لحظه برای آنها پاسخگویی کرد. گم شدن یا به سرقت رفتن این دستگاه‌ها را باید به مدیریت گزارش داد.

### ۳.۲.۲ - مدیریت کارکنان

مدیر آزمایشگاه یا پژوهشگر ارشد، اداره کارمندان را که مواد، دستگاه‌ها و تجهیزات زیربنایی محل را همه روزه به کار می‌برند، برعهده دارند. رهبری و مدیریت خوب هم برای ایمنی زیستی و هم برای امنیت زیستی از اهمیت ویژه برخوردار است، زیرا مدیر آزمایشگاه یا پژوهشگر ارشد حقوق و وظایف کارمندان را در دسترسی به مواد خطرناک تعیین می‌کند و مسئولیت‌ها بر پایه صلاحیت‌های حرفه‌ای، صلاحیت‌های امنیتی و سوابق کاری تقسیم می‌شوند. آموزش و تمرین همراه با رهبری درست در ایجاد یک گروه کارآمد از همکاران و پرهیز از اختلافات اهمیت حیاتی دارد. یکی از خطرهای مورد بحث عامه عبارت است از تهدید "داخلی" که توسط شخصی بروز می‌کند که هم به مواد دسترسی دارد و هم به دانش فنی لازم برای آنکه مواد را پنهانی بردارد و برای مقاصد مخرب به کار ببرد. برای رویارویی با اینگونه خطرها، مدیریت کارکنان باید برای کشف و اداره



تصویر شماره ۳: پژوهشگری با تمام تجهیزات در آزمایشگاه BSL4



اختلافات پیش از آن که در دسری برای ایمنی و امنیت شوند، راهبردهایی را به کار بندد. ایجاد و حفظ روابط حرف‌های خوب با کارمندان در پیشگیری از چنین وضعیت‌هایی مؤثر است.

#### ۳.۲.۲.۱. امنیت پیش از استخدام

پیش از دعوت از یک کارمند احتمالی برای مصاحبه، باید صحت کارنامه‌ها و تجربه او از کارهای پیشین ارزیابی شود تا نسبت به توانایی‌های او اطمینان حاصل شود. باید از کارفرمایان پیشین او توصیه‌نامه خواست و مدارک دانشگاهی او را به تأیید رساند. جستجو در اینترنت می‌تواند اطلاعات بیشتری درباره کارمند تازه احتمالی به دست دهد و پرسش‌هایی را پیش آورد که می‌توان هنگام مصاحبه استخدامی از او پرسید.

اگر قرار باشد برای کارمند تازه اجازه دسترسی به مواد با خطر بالا و آزمایشگاه‌های با سطح حفاظتی بالا (BSL3 و BSL4) صادر شود، شاید بررسی عمیق‌تر سوابق او (تأیید صلاحیت امنیتی) لازم شود. این قبیل بررسی‌ها مستلزم کمک گرفتن از کارشناسان امنیتی و کارکنان مجری قانون است و باید توسط مدیریت سازمان در مشورت با مدیر آزمایشگاه یا متصدی ایمنی زیستی و امنیت زیستی به عمل آید.

#### ۳.۲.۲.۲. تقسیم وظایف

پیش از آنکه به یک کارمند جدید اجازه دسترسی به بخش‌های ممنوعه داده شود، سرپرست مربوطه باید به دقت برآورد کند که تا چه سطحی به این کارمند استقلال و اجازه دسترسی به اطلاعات بدهد. در آغاز باید دسترسی محدود به بخش‌هایی باشد که برای انجام کار کارمند تازه لازم هستند و محدود به آن جاهای نگهداری باشند که مواد لازم برای کار او در آنها جای داده شده است. در طول دوره مقدماتی، مدیر آزمایشگاه یا پژوهشگر ارشد شاید بخواهند که به شخصه کارمند تازه را سرپرستی کنند و دسترسی به مواد و بخش‌ها را به شرط حضور سرپرست اجازه دهند تا تأیید شود و کار با ایمنی و امنیت صورت بگیرد.

در یک فرهنگ مشتمل بر مسئولیت، مسئولیت‌های هر کارمند به عنوان عضوی از تیم تعریف می‌شود و آگاهی بر موارد امنیتی در او پرورانده می‌شود. تقسیم مسئولیت‌ها باید با توانایی‌های اعضای تیم خوانایی داشته باشد و این تقسیم باید به طور مرتب توسط مدیر آزمایشگاه یا سرمحقق مورد تجدید نظر قرار بگیرد.

#### ۳.۲.۲.۳ - حق دسترسی و مسئولیت کارمند

دسترسی به بخش‌های ممنوعه باید بر پایه نیاز و صلاحیت کارمند باشد. مدیر آزمایشگاه یا پژوهشگر ارشد باید میزان استقلال لازم برای یک کارمند را در نظر داشته باشند و عواملی از این قبیل را به حساب آورند که کارمند چه ساعت‌هایی و به چه بخش‌هایی اجازه دسترسی داشته باشد (برای مثال به فریزرها و اتاق دستگاه‌ها و آزمایشگاه‌های حفاظت شده). کارمندی که به آزمایشگاه‌ها و مواد BSL1 و BSL2 دسترسی دارند، باید اجازه دسترسی به بخش‌های ممنوعه را داشته باشند. لازمه دسترسی کامل به آزمایشگاه‌های BSL3 و BSL4 داشتن اجازه دسترسی به بخش‌های مطلقاً ممنوع است. یک راهبرد معمول که هم برای رعایت ایمنی و هم برای پیشگیری از تهدید داخلی به کار می‌رود عبارت است از «قانون دو نفر» که بر اساس آن هیچ شخصی به تنهایی اجازه دسترسی مستقل



به BSL3 و BSL4 را ندارد. ممنوعیت‌هایی برای کارهای بیرون از چهارچوب طبقه‌بندی BSL نیز می‌توان وضع کرد، از قبیل تولید یا کاری که با حیوانات سروکار دارد. حق دسترسی را باید مرتب مورد ارزیابی مجدد قرار داد و در صورت عدم نیاز آن را باطل کرد. سهل‌انگاری و رفتار بی‌دقت که ایمنی یا امنیت را به خطر می‌اندازد باید مورد رسیدگی قرار گیرد و حق دسترسی باید لغو شود یا اگر درخواست شد، رد شود. با پایان استخدام، جا دارد که روش درستی وجود داشته باشد که به آن طریق بتوان حق دسترسی و سایر امتیازهای مربوط به کار را به‌موقع لغو کرد، کارت‌های شناسایی را پس گرفت و کارت‌های ورودی را باطل کرد. در مورد میهمانانی که به آنها اجازه ورود به ساختمان یا آزمایشگاه داده می‌شود، باید دقت ویژه‌ای به عمل آورد. جنبه‌های امنیتی صدور اجازه ورود میهمان به آزمایشگاه باید از پیش بررسی شود و میزبان باید در تمام مدت مسئول ایمنی و رفتار او باشد.

#### ۳.۲.۲.۴ - مدیریت اختلافات

برای تحقق یک محیط کار ایمن، باید اختلاف‌ها و سایر مسائل میان کارکنان را که می‌تواند در کار تأثیر بگذارند شناسایی شوند و مورد توجه قرار بگیرند (بخش‌های پیشین را نیز بنگرید). اینگونه مسائل ممکن است در میان همکاران، یا میان کارکنان و مدیریت بروز کند، یا آنکه منشاء شخصی داشته باشد. از جمله مواردی در ارتباط با نکات زیر را میتوان نام برد:

- دستمزد یا مسائل اقتصادی
- رقابت
- کنار گذاشته شدن از جمع
- سلامت روانی
- زندگی خصوصی

صرف نظر از ماهیت این مشکلات، مهم آن است که به‌موقع و پیش از آنکه از کنترل خارج شوند، کشفشان کرد.

بگومگوی میان کارکنان یا مشکلات شخصی بیرون از محل کار، بالقوه می‌تواند به بروز تهدید داخلی بی‌انجامد. احتمال بروز چنین خطری را مشکل می‌توان کشف کرد، به‌ویژه اگر منشاء آن نارضایتی‌های بیرون از محل کار باشد. مدیر آزمایشگاه یا پژوهشگر ارشد باید در قبال کارکنان حساس باشند و بکوشند که مشکلات را زود شناسایی کنند و وسایل لازم را برای حل مشکل فراهم کنند؛ از قبیل مشاوره یا میانجیگری. کارمندان در صورت نیاز باید به کمک یا مشاوره دسترسی داشته باشند.

#### ۳.۲.۳ - مدیریت اطلاعات

##### ۳.۲.۳.۱ - انواع اطلاعات حساس

حفاظت از اطلاعات حساس به اندازه محدودیت دسترسی به مواد پرخطر اهمیت دارد. دسترسی به اطلاعات حساس باید محدود به آن عده از کارمندان باشد که آن را برای کارشان لازم دارند. اطلاعات حساس اغلب اطلاعاتی است که میتواند توسط فرد سوء استفاده‌گر و برای دستیابی به امکانات و

مکان‌هایی که مواد بیولوژیک پرخطر در آنها نگهداری می‌شوند به کار رود (بنگرید به بخش ۲.۳.۵). اینها عبارت هستند از اطلاعاتی درباره:

- عوامل عفونی و سموم
- مکان‌های نگهداری
- رمزهای ورودی
- حفاظت فیزیکی
- روش‌های حفظ امنیت

سایر اطلاعات مربوط به اموال آزمایشگاه یا کارمندان نیز می‌تواند برای برخی گروه‌ها ارزشمند باشد و باید از آنها حفاظت کرد. فرد سوء استفاده‌گر و بزه‌کار، می‌تواند از اطلاعات مربوط به یک کارمند، برای فشار آوردن به او استفاده کند. مثلاً او را وادار به سرقت اطلاعات و مواد کند یا از طریق او، خود به امکانات اطلاعاتی دسترسی پیدا کند. اینگونه اطلاعات شامل موارد زیر است:

- جزئیات استخدامی
- پرونده پزشکی
- نام کارمندانی که با حیوانات آزمایشگاهی سروکار دارند
- مکاتبات کارکنان از طریق ایمیل

نوع سومی از اطلاعات را نیز باید تحت حفاظت ویژه قرار داد. این نوع اطلاعات را نباید در دسترس سایر کارمندان یا غیر کارمندان قرار داد. این اطلاعات عبارت هستند از:

- اطلاعات منتشر نشده آزمایش‌ها
- اطلاعات مربوط به مالکیت بر امتیاز
- درخواست ثبت امتیاز
- صورت جلسات داخلی
- پرونده بیماران که اغلب قوانین کشوری نیز از آنها حفاظت می‌کند.

### ۳.۲.۳.۲ - حراست از اطلاعات حساس

تعیین آن که چه اطلاعاتی را باید حساس نامید خود چالش دشواری است. نویسنده اطلاعات (به‌طور معمول مدیر آزمایشگاه یا پژوهشگر ارشد) باید تصمیم بگیرد که آیا اطلاعات باید حساس شمرده شوند یا نه. نویسنده باید مشخص کند اطلاعات چگونه باید حفاظت شوند و چه کسانی به آن دسترسی داشته باشند. نویسنده همچنین باید تصمیم بگیرد که در چه زمانی این اطلاعات دیگر حساس شمرده نمی‌شوند یا می‌توان آنها را نابود کرد.<sup>[۳۳]</sup> روش اخیر کمک می‌کند که اطلاعات حساس در حد مورد نیاز نگه‌داشته شوند و بتوان آنها را کنترل کرد.

از اطلاعات حساس باید با روش‌های سنجیده‌ای برای تولید، بایگانی، جابه‌جایی و نابود کردن نسخه‌های فیزیکی یا الکترونیکی آن محافظت کرد. در صورت نیاز باید از رمزنویسی استفاده کرد. امکانات کپی‌برداری backup کافی نیز باید فراهم شود و باید تضمین کرد که اطلاعات برای همیشه از دست نمی‌رود و خراب نمی‌شود.



### ۳.۳- فوریت‌های امنیت زیستی

با وجود مدیریت مؤثر، بازهم ممکن است خطرها، فوریت‌ها یا وضعیت‌های پیش‌بینی نشده‌ای رخ دهد. برای رویارویی مناسب با چنین وضعیت‌هایی باید طرح‌هایی قابل اجرا وجود داشته باشد. برنامه‌ریزی برای فوریت‌ها یا وضعیت‌های پیش‌بینی نشده بخشی جدایی‌ناپذیر از امنیت زیستی کاربردی است. هر آزمایشگاهی باید روش‌هایی برای ارزیابی وضعیت‌های غیرعادی بی‌اندیشد و معیارهایی داشته باشد برای آن که تعیین کند در چه موقعیت‌هایی دخالت از خارج آزمایشگاه موجه است. برخی حوادث امنیتی ممکن است مستلزم دخالت مراجع قانونی باشد و به تحقیقات جنایی منجر شود.

تقاضای کمک از بیرون در موارد زیر پیش می‌آید:

- خسارات مالی وارد شده باشد.
- کارکنان آسیب دیده باشند.
- تهدیدی صورت گرفته باشد.
- اموالی به سرقت رفته باشد.

#### ۳.۳.۱- برنامه‌ریزی واکنش

واکنش نسبت به نقض امنیت زیستی یا حوادث باید در بردارنده روش‌هایی باشد که جنبه‌های گوناگون این رخدادها را در نظر بگیرد. طرح‌های ناظر بر احتمال وقوع این قبیل فوریت‌ها یا وضعیت‌های پیش‌بینی نشده باید موارد زیر را در بر بگیرد:

- خسارت مالی
- آسیب‌دیدگی کارکنان
- سرقت یا از دست رفتن اموال به شکل دیگر از جمله لو رفتن رمزهای ورودی، از کف دادن کارت‌های شناسایی و مانند آنها
- اختلاف در صورت موجودی‌ها
- تلاش موفق یا ناموفق دسترسی غیر مجاز (فیزیکی یا الکترونیکی)
- خشونت و تهدید
- رفتار مشکوک یا سهل‌انگارانه

طرح واکنش باید رئوس روشی را که اجرای آن لازم است به‌روشنی برشمارد. هدف از آن باید ایجاد شیوه کارآمد رساندن اطلاعات مهم به همه کارمندان و مقامات مربوطه باشد. این طرح باید دربرگیرنده موارد زیر باشد:

- روش‌هایی برای ارزیابی شدت حادثه به منظور تعیین اقدام مناسبی که باید صورت بگیرد.
- نام کارمند دارای مقام سرپرستی (یعنی مدیر آزمایشگاه، پژوهشگر ارشد، یا متصدی ایمنی زیستی و امنیت زیستی).
- شمای نقش و مسئولیت افراد، از جمله در طول ساعت‌های غیر اداری.
- نقشه و دیگر اطلاعات لازم درباره محدوده آزمایش، ساختمان، یا آزمایشگاه.
- روال کار در موارد فوریت برای تخلیه ایمن و حمل و نقل و جابه‌جایی تلفات.
- روش‌هایی برای زدودن مواد خطرناک و روش‌های آلودگی‌زدایی کامل.

- اطلاعات درباره کارکنان مسئول فوریت‌ها و مراجع قانونی محلی.
- سایر اطلاعات لازم برای تماس.

### ۳.۳.۲ - گزارش نقض امنیت یا رخداد‌های امنیتی

یک سیستم قابل اعتماد الکترونیکی یا فیزیکی باید وجود داشته باشد که به آسانی در دسترس باشد و درست کار کند تا در صورت لزوم بتوان موارد نقض امنیت یا رخداد‌های امنیتی را گزارش داد. چنین سیستمی بستگی به تمایل گزارش رویدادها صرف نظر از شدت و عواقب آنها دارد. نقض اصول و رخداد‌های امنیتی اغلب گزارش داده نمی‌شوند زیرا وضعیت به خوبی اداره و حل و فصل می‌شود. نقض اصول و رخداد‌های امنیت زیستی همچنین ممکن است به دلیل شرمساری از وقوع آن یا به دلیل ترس از مبالغه در وضعیت پیش‌آمده گزارش داده نشوند.

کوتاهی در گزارش یک حادثه اما به معنی آن است که درسی که می‌شد از آن گرفت، از دست می‌رود. رخداد‌های مربوط به امنیت زیستی که در نشریات علمی منتشر شده‌اند به‌طور عمده آنهایی هستند که در ایالات متحده آمریکا روی داده‌اند، زیرا در این کشور مقررات سختی بر کاربرد و جابه‌جایی مواد بیولوژیک حاکم است و ایمنی زیستی و امنیت زیستی به‌طور علنی موشکافی شده است. کمبود اطلاعات درباره رخداد‌های مشابه در دیگر کشورها و درباره درس‌هایی که می‌توان از آنها آموخت، پیشگامان امنیت زیستی در این کشورها را در موضع ضعف قرار می‌دهد و ممکن است از آن رو باشد که به گزارش این قبیل حوادث اهمیت لازم داده نمی‌شود.

### ۳.۴ - تمرین و ارزیابی

ارزیابی پیوسته و بازبینی روشها و آیین‌نامه‌ها از عوامل مهم برقراری سطح بالایی از امنیت زیستی است. روش‌های مربوط به کار با عوامل عفونی و سموم ممکن است در طول زمان دستخوش تغییر شوند. این تغییرات، به اضافه تغییرات در انبار مواد، محل نگهداری و دسترسی به مواد، باید به‌موقع به کارمندانی که مسئولیت امنیت را دارند اطلاع داده شود. اگر قرار است صحت اطلاعات و پاسخ‌گویی برقرار باشد، باید به کارمندان اطلاعات داده شود. چنین روش‌هایی همچنین گزارش سریع رخدادها را امکان‌پذیر می‌سازد و به هریک از کارمندان کمک می‌کند در زمینه امنیت زیستی و مسئولیت شخصی هشیاری داشته باشد.

بازرسی و معاینه به منظور کسب اطمینان برای رعایت اصول از ابزارهای مهم برقراری امنیت زیستی است. شرکت در تمرین و مانورهای واکنش به فوریت‌ها نیز به ایجاد آگاهی بر اهمیت امنیت زیستی کمک می‌کند.

این تمرین‌ها کمک می‌کند که نقش هر یک از کارمندان تعریف و همزمان نقاط ضعف او در آمادگی‌های لازم آشکار شود.



## واژه‌نامه

منظور اطلاعاتی است که احتمال استفاده افراد بزهکار از آن‌ها به منظور دسترسی به امکانات و مکان‌های حاوی مواد بیولوژیک پر خطر وجود دارد. برای نمونه می‌توان به فهرست عوامل عفونی و سموم، محل نگهداری آنها، رمزهای ورودی، روال امنیتی و جزئیات حفاظت فیزیکی و حفاظت از روند کار اشاره کرد.

### اطلاعات حساس

ADR موافقت‌نامه اروپا درباره حمل و نقل بین‌المللی محموله‌های خطرناک در جاده‌ها در ۳۰ سپتامبر ۱۹۵۷ برای امضا ارائه شد و در ۲۹ ژانویه ۱۹۶۸ به مورد اجرا گذاشته شد. هدف از آن افزایش ایمنی حمل و نقل بین‌المللی محموله‌های خطرناک در جاده‌ها است و چگونگی حمل و نقل بین‌المللی محموله‌های خطرناک را شرح می‌دهد.

### آدی آر

Risk assessment روند شناسایی سرچشمه آسیب‌های احتمالی در پیوند با امکان گم شدن، سرقت، دسترسی غیر مجاز، سوءاستفاده، اشاعه عمدی یا سهوی عوامل عفونی یا سموم به هنگام نگهداری، استفاده با مقاصد قانونی، جابه‌جایی و تحویل دادن آنهاست. همچنین شامل برآورد امکان بروز این آسیب‌ها و میزان آسیب‌های کوتاه‌مدت و بلندمدت است.

### برآورد خطر

سطوح ایمنی ۱ تا ۴ که میزان حفاظت لازم برای کار ایمن و امن با بیمارگرهای معین یا سموم را تعریف می‌کند. BSL1 پایین‌ترین سطح حفاظت و BSL4 بالاترین سطح آن است.

### BSL

پیمان منع گسترش، تولید، و انباشت سلاح‌های باکتریایی (بیولوژیک) و سمی و نابودسازی آن‌ها (کنوانسیون سلاح‌های بیولوژیک و سمی) در تاریخ ۱۰ آوریل ۱۹۷۲ برای امضا ارائه شد و در ۲۶ مارس ۱۹۷۵ قدرت اجرایی یافت. این پیمان گسترش، تولید، انباشت، دست‌یابی به شکلی دیگر و نگهداری عوامل میکروبی یا دیگر عوامل بیولوژیک یا سمی را صرف نظر از منشأ یا شیوه تولید انواع آن و به مقادیری که هیچگونه توجیه پیشگیری از بیماری، حفاظتی یا نیت‌های صلح‌آمیز بر آن متصور نباشد را منع می‌کند. نیز سلاح‌ها، دستگاه‌ها یا وسایل توزیع ساخته‌شده برای استفاده از این

### BTWC

عوامل یا سموم را برای نیات خصمانه یا مناقشات مسلحانه منع می‌کند.

**Bioterrorism** اعمال خشونت با عوامل بیولوژیک یا سموم و همچنین تهدید به استفاده از آن برای پیش بردن یک نیت سیاسی یا مقابله با ارزش‌های دموکراتیک است.

### تروریسم بیولوژیک

**Insider threat** فردی با حق دسترسی به امکانات (یعنی یک کارمند یا کاربر مجاز) که به عمد یا به اجبار اموال سازمان را خود برای مقاصد مخرب به کار می‌برد یا در اختیار کسی دیگر می‌نهد.

### تهدید داخلی

**Containment** جدا داشتن مواد پر خطر به منظور جلوگیری از آسیب زدن به انسان‌ها، حیوانات، گیاهان و محیط زیست.

### حفاظت

**Dual use** مواد، اطلاعات یا فناوری‌هایی که بیش از یک مورد مصرف دارند و می‌توانند به شیوه‌ای زیان‌بار مورد سوءاستفاده قرار گیرند.

### کاربرد دوگانه

**Biosafety** اصول، فناوری‌ها و روش‌هایی که برای پیشگیری از ابتلا یا پخش کردن اتفاقی یا غیر عمدی بیمارگرها و سموم ایجاد شده است.

### ایمنی زیستی

**Biosecurity** اصول، فناوری‌ها و روش‌هایی که برای حفاظت عوامل عفونی، سموم و فناوری حساس در مقابله با دسترسی غیر مجاز، گم شدن، به سرقت رفتن، سوءاستفاده، و اشاعه عمدی یا سهوی آن‌ها ایجاد شده است.

### امنیت زیستی

**Principal investigator** پژوهشگر کلیدی مانند دانشمند ارشد، رهبر گروه یا مدیر آزمایشگاه که نگهبان اصلی مواد بیولوژیک، دستگاه‌ها و اطلاعات حساس است.

### سرمحقق

**Severity** اصطلاحی در برآورد خطر احتمالی یا خسارت وارد شده از سوی یک عامل بیولوژیک یا سم است.

### شدت

**Risk management** به اجرا گذاشتن روش‌ها و شیوه‌هایی برای کاهش خطر تا میزان قابل قبول است.

### مدیریت خطر

WHO سازمان بهداشت جهانی



## پی‌نوشت‌ها:

۱- این تعریف از سازمان بهداشت جهانی (WHO)

Biorisk Management: Laboratory Biosecurity Guidance (WHO: Geneva, Sep. 2006), <[http://www.who.int/resources/publications/biosafety/WHO\\_CDS\\_EPR\\_2006\\_6/en/](http://www.who.int/resources/publications/biosafety/WHO_CDS_EPR_2006_6/en/)>, صفحه‌های ۶۸،

سازمان گسترش و همکاری های اقتصادی (OECD)، اداره علوم، فناوری و صنایع،

Best Practice Guidelines on Biosecurity for Biological Resource Centres (OECD: Paris, 2007), <<http://www.oecd.org/>>, صفحه ۸،

و دبیرخانه ابتکار گسترش استاندارد جهانی خطر بیولوژیک،

'Laboratory biorisk management standard, CWA biorisk public enquiry', 25 July 2007, <[http://www.biorisk.eu/documents/draft\\_document.PDF](http://www.biorisk.eu/documents/draft_document.PDF)>, صفحه‌های ۷-۱۳،

Comité Européen de Normalisation مخفف CEN است. CWA مخفف پیمان کارگاه CEN است. کمیته اروپایی استاندارد (ها) است.

۲- رهنمود EEC/۹۰/۲۱۹ شورا به تاریخ ۲۳ آوریل ۱۹۹۰ پیرامون استفاده کنترل شده از میکروارگانیسم‌های دستکاری شده، Official Journal of the European Communities, L117, 8 May 1990؛ رهنمود EC/۲۰۰۰/۵۴ صادره از پارلمان اروپا و شورای ۱۸ سپتامبر ۲۰۰۰ پیرامون حفاظت از کارگران در برابر خطرهای ناشی از قرار گرفتن در معرض عوامل بیولوژیک در کار، Official Journal of the European Communities, L262, 17 Oct. 2000؛ و رهنمود EC/۲۰۰۱/۱۸ شورا صادره از پارلمان اروپا و شورای ۱۲ مارس ۲۰۰۱ پیرامون اشاعه عمدی ارگانیسم‌های بازن‌های دست‌کاری شده در محیط زیست، و رهنمود العایی EEC/۹۰/۲۲۰/EEC شورا، Official Journal of the European Communities, L106, 17 Apr. 2001. همچنین یادداشت شماره ۱ را بنگرید.

۳- سازمان گسترش و همکاری‌های اقتصادی (یادداشت ۱)؛ سازمان بهداشت جهانی (یادداشت ۱)؛ وزارت بهداشت و خدمات انسانی ایالات متحده، مرکز بازاری و پیشگیری بیماری‌ها و انستیتوی ملی بهداشت،

Biosafety in Microbiological and Biomedical Laboratories, 5th edn (US Government Printing Office: Washington, DC, 2007)؛ A Code of Conduct for Biosecurity: Report by the Biosecurity Working Group (Royal Netherlands Academy of Arts and Sciences: Amsterdam, Aug. 2008)؛ و کمیته اروپایی استاندارد (ها) 'Laboratory biorisk management standard', CEN Workshop Agreement CWA15793, Feb. 2008, <<ftp://ftp.cenorm.be/PUBLIC/CWAs/wokrshop31/CWA15793.pdf>>.

۴- متن BTWC در نشانی <<http://www.opbw.org/convention/documents/btwctext.pdf>> در دسترس است. ماده ۴ BTWC را بنگرید؛ و قطعنامه شماره ۱۵۴۰ شورای امنیت سازمان ملل متحد، ۲۸ آوریل ۲۰۰۴، ماده ۳.

۵- تعریف از سازمان بهداشت جهانی (یادداشت ۱)، ص ۴

۶- سازمان بهداشت جهانی (یادداشت ۱)، صص ۱۴-۱۳



۷- وزارت بهداشت و خدمات انسانی ایالات متحده (یادداشت ۳)

۸- رهنمود EC/2000/54 (یادداشت ۲)

۹- ر.م. سالرنو و ج. گائودیوزو

R. M. Salerno and J. Gaudio, Laboratory Biosecurity Handbook (CRC Press: Boca Raton, FL, 2007), صفحه ۱۶.

۱۰- S. W. Carus, 'Bioterrorism and biocrimes: the illicit use of biological agents since 1900'

تیز پژوهشی، مرکز پژوهش مبارزه با گسترش سلاح‌ها، دانشگاه دفاع ملی، واشینگتن دیسی، فوریه ۲۰۰۱، صص ۴۵-۴۳، ۶۱.

۱۱- ایمنی زیستی درجه ۱ تا ۴ میزان حفاظت لازم برای کار ایمن و امن با بیمارگرها و سموم معین را مشخص می‌کند.

۱۲- دستورالعمل‌های اتحادیه اروپا برای امنیت زیستی آزمایشگاه‌ها هنوز قطعی نشده و بنابراین برآورد کامل امنیت زیستی

ممکن نیست و بیرون از چهارچوب این کتابچه راهنما قرار می‌گیرد.

۱۳- سازمان بهداشت جهانی (یادداشت ۱)، ص ۲۳.

۱۴- سالرنو و گائودیوزو (یادداشت ۹)، ص ۵۱.

۱۵- سازمان بهداشت جهانی (یادداشت ۱)، ص ۱۹.

۱۶- دبیرخانه ابتکار گسترش استاندارد جهانی خطر بیولوژیک (یادداشت ۱)، ص ۴۶. «کارمندان باید از کاربرد عامل بیولوژیک

زیان‌بخشی که بنا بر ماهیت کار می‌توان آن را جایگزین کرد بپرهیزند و آن را با عامل بیولوژیک دیگری که در شرایط کاربرد آن،

بر حسب مورد، و مطابق با دانش موجود، خطرناک نیست یا خطر کمتری برای بهداشت کارمند دارد، جایگزین کنند.» رهنمود

EC/2000/54، ماده ۵ (جایگزینی).

۱۷- Australia Group, 'Control list of dual-use biological equipment and related technology',

<[http://www.australiagroup.net/en/dual\\_biological.html](http://www.australiagroup.net/en/dual_biological.html)>.

۱۸- سازمان گسترش و همکاری‌های اقتصادی (یادداشت ۱)، صص ۱۱-۱۰، ۱۶.

۱۹- سازمان بهداشت جهانی (یادداشت ۱)، ص ۲۷.

۲۰- کمیته اروپایی استانداردها (یادداشت ۳)، ص ۴۵.

۲۱- دبیرخانه ابتکار گسترش استاندارد جهانی خطر بیولوژیک (یادداشت ۱)، ص ۴۱؛ و سازمان بهداشت جهانی

(یادداشت ۱)، ص ۲۲. همچنین بنگرید به موافقتنامه اروپا درباره حمل و نقل بین‌المللی محموله‌های خطرناک در جاده‌ها

(Accord européen sur le transport des marchandises dangereuses par route, ADR). این موافقتنامه

در ۳۰ سپتامبر ۱۹۵۷ برای امضا ارائه شد و در ۲۹ ژانویه ۱۹۶۸ به مرحله اجرا در آمد. تازه‌ترین اصلاحیه‌های آن در ۱ ژانویه

۲۰۰۹ به اجرا گذاشته شد. نسخه بازنویسی شده و یک جای آن به عنوان سند ECE/TRANS/202، جلد‌های ۱ و ۲ (ADR 2009)

منتشر شد <<http://www.unece.org/trans/danger/publi/adr/adr2009/09ContentsE.html>>.

۲۲- سازمان گسترش و همکاری‌های اقتصادی (یادداشت ۱)، ص ۱۴

۲۳- ADR را بنگرید (یادداشت ۲۱).

۲۴- تارنمای PubMed را بنگرید، <<http://www.ncbi.nlm.nih.gov/PubMed>>.

۲۵- کمیته اروپایی استانداردها (یادداشت ۳)، ص ۲۹.

۲۶- آیین‌نامه EEC/3381/94 شورا پیرامون کنترل صادرات محموله‌های دو کاربردی،

Official Journal of the European Communities, L367, 31 Dec. 1994، ص ۱.

۲۷- آیین‌نامه شورا (EC) شماره ۲۸/۲۰۰۹ به تاریخ ۵ مه ۲۰۰۹ پیرامون ایجاد سازمانی برای کنترل صادرات، جابه‌جایی، واسطه‌گری و

عبور و مرور اقلام دو کاربردی، Official Journal of the European Union, L134, 29 May 2009.

۲۸- متن پیمان در این نشانی در دسترس است: <<http://www.opbw.org/convention/conv.html>>.



۲۹- قطعهنامه شماره ۱۵۴۰ شورای امنیت سازمان ملل متحد (یادداشت ۴).

۳۰- دیوان پاسخگویی دولت امریکا

(GAO) High-Containment Biosafety Laboratories: Preliminary Observations on the Oversight of the Proliferation of BSL 3- and BSL 4- Laboratories in the United States, GAO 108- 08-T (GAO: Washington, DC, 4 Oct. 2007).

۳۱- آژانس بهداشت عمومی کانادا

Laboratory Biosafety Guidelines, 3rd edn (Public Works and Government Services: Ottawa, 2004), صفحه ۲۷.

۳۲- بنگرید به تارنمای گروه استرالیا، <<http://www.australiagroup.net>>. شرکت‌کنندگان کنونی در گروه استرالیا عبارتند از: آرژانتین، آلمان، اتریش، اسپانیا، استرالیا، استونی، اسلواکی، اسلونی، انگلستان، اوکراین، ایالات متحده، ایتالیا، ایرلند، ایسلند، بلژیک، بلغارستان، پرتغال، ترکیه، جمهوری چک، دانمارک، رومانی، ژاپن، سوئد، سوئیس، فرانسه، فنلاند، قبرس، کانادا، کرواسی، کره جنوبی، لتونی، لوکزامبورگ، لهستان، لیتوانی، مالت، مجارستان، نروژ، نیوزیلند، هلند، یونان، و کمیسیون اروپا.

۳۳- سالرنو و گائودیوزو (یادداشت ۹)، ص ۵۸.

## درباره نویسندگان

دکتر پیتر کلهوستیگ (Peter Clevestig سوئد) پژوهشگر ارشد پروژه امنیت شیمیایی و بیولوژیک برنامه کنترل و عدم گسترش تسلیحات سیپری SIPRI است. او در زمینه ویروس‌شناسی تجربه دارد و پیش از پیوستن به سیپری در بخش میکروبیولوژی و بیولوژی غدد و سلول‌ها در بنیاد کارولینسکا (KI) استکهلم، پژوهش می‌کرد. این پژوهشگر همچنین به عنوان رئیس کمیته زیست‌ایمنی KI خدمت می‌کرد و عضو فعال شبکه زیست‌ایمنی اسکاندیناوی Nordic Biosafety Network و انجمن زیست‌ایمنی اروپا (European Biosafety Association EBSA) نیز است. دکتر پیتر کلهوستیگ مطالب علمی متعددی به‌طور عمده در زمینه ویروس‌شناسی نوشته یا در نوشتن آنها همکاری داشته و به‌طور منظم در واحدهای پژوهش‌های علمی اروپا در موضوع امنیت زیستی تدریس می‌کند.

دکتر علی کریمی Ali Karami پژوهشگر و دانشیار رشته بیولوژی مولکولی عضو هیئت علمی مرکز تحقیقات بیولوژی مولکولی دانشگاه علوم پزشکی بقیه‌الله در تهران - ایران است. او مقالات علمی بسیاری در نشریات بین‌المللی و ملی منتشر کرده و صاحب نظر در زمینه‌های مختلف بیوتکنولوژی، بیولوژی مولکولی، اخلاق و حقوق زیستی، ایمنی زیستی و حفاظت زیستی است.



**STOCKHOLM INTERNATIONAL  
PEACE RESEARCH INSTITUTE**

Signalistgatan 9  
SE-169 70 Solna, Sweden  
Telephone: +46 8 655 97 00  
Fax: +46 8 655 97 33  
Email: sipri@sipri.org  
Internet: www.sipri.org

## راهنمای امنیت زیستی کاربردی برای آزمایشگاه‌های علوم زیستی

زیست‌امنیت طیف گسترده‌ای از خطرها و تهدیدهای بالقوه، از فعالیت‌های بزهکارانه تا تروریسم بیولوژیک و جاسوسی را در بر می‌گیرد. این کتابچه راهنما روی فعالیت‌های آزمایشگاهی و اجزای اصلی زیست‌امنیت کاربردی که برای همه کارمندان آزمایشگاه‌ها مصداق دارند، متمرکز شده‌است. نقش مدیران آزمایشگاه‌ها و سرمحققان در حراست از اموال آزمایشگاه و کارمندان زیر سرپرستی آنان نیز مورد توجه قرار گرفته‌است.

این کتابچه حاوی دستورالعمل‌هایی است برای کارکنانی که با بیمارگرهای واگیردار و سمومی کار می‌کنند که ممکن است بهداشت انسان‌ها، حیوانات، و گیاهان را تحت تأثیر قرار دهند. هدف از این راهنما علاقمند کردن دانشمندان، کارکنان آزمایشگاه‌ها، و دانشجویان به زیست‌امنیت آزمایشگاهی، و ارائه‌ی راهنمایی‌های عملی است که به کار بردن و نگهداری ایمن مواد بیولوژیک را تضمین می‌کند.

اذعان داشتن بر خطرهای زیست‌امنیتی و نقش پر اهمیت کارمندان در برقراری زیست‌امنیت، برای تأمین ایمنی و امنیت محیط کار ضرورت دارد. حراست از عوامل آلوده‌کننده همچنین بنا به قانون وظیفه‌ای ملی است و در کنوانسیون ۱۹۷۲ سلاح‌های بیولوژیک و سمی و قطعنامه شماره ۱۵۴۰ شورای امنیت سازمان ملل متحد درج شده‌است.

ISBN 978-91-85114-68-9



9 789185 114689