

# Safety Management System (SMS) Documents and Records Control

NIST S 7101.15

Approval Date: 06/14/2023

Effective Date: 06/14/2023<sup>1</sup>

## 1. PURPOSE

The purpose of this suborder is to establish requirements and associated roles and responsibilities needed to ensure the documents and records used to implement and comply with the NIST Safety Management System (SMS) are appropriately controlled and managed.

## 2. BACKGROUND

As established by NIST P 7100.00: *Occupational Safety and Health*, NIST P 7300.00: *Environmental Management* and NIST P 7400.00: *Fire and Life Safety (FLS)*, it is NIST policy to carry out all activities in a manner that protects human health and the environment. To effectively implement these three policies, OSHE has implemented a SMS, as defined by the NIST Orders associated with these policies. Two cornerstones of accomplishing this implementation are:

- Ensuring documents are accurate and controlled, by implementing processes to ensure:
  - Documents are uniquely identifiable via a standard nomenclature;
  - Documents are reviewed and approved prior to use;
  - Documents are updated as necessary using a controlled process;
  - Revisions are documented;
  - Current versions are legible, identifiable and available;
  - Obsolete documents are not used; and
  - External documents are identified and managed;
  
- Ensuring records are managed such that they are identifiable, complete, legible, readily retrievable, and stored in a manner that protects them from damage or loss.

---

<sup>1</sup> For revision history, see Appendix A.

37 This suborder establishes document and record control requirements of the NIST SMS, EMS  
38 and FLS.

39  
40

41 **3. APPLICABILITY**

42 a. The provisions of this suborder apply to internal and external documents and records used to  
43 comply with the requirements of the NIST SMS, EMS and FLS program except as noted in  
44 Section 3.b<sup>2</sup>.

45

46 b. The provisions of this suborder do not apply to OU documents and records maintained by  
47 OUs to comply with requirements established in SMS documents.

48

49

50 **4. REFERENCES**

51 a. NIST O 1110.00: *Directives Management System*

52

53 b. NIST PR 1000.05: *Forms Management*

54

55 c. NIST O 1601.00: *Records Management*

56

57 d. OPBM-NP-18-0001 United States Department of Commerce (DOC) Controlled Unclassified  
58 Information (CUI) Policy, August 14, 2019 (DOC CUI Policy)

59

60 e. OPBM-NP-18-001 U.S. Department of Commerce Controlled Unclassified Information  
61 (CUI) Guidelines, August 2019 (DOC CUI Guidelines)

62

63 f. [National Archives and Records Administration General Records Schedule](#)

64

65

66 **5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH DIRECTIVES**

67 a. NIST P 7100.00: *Occupational Safety and Health*

68

69 b. NIST P 7300.00: *Environmental Management*

70

71 c. NIST P 7400.00: *Fire and Life Safety*

72

---

<sup>2</sup> Documents and records used to comply with the requirements of NIST O 7200.00: *Ionizing Radiation Safety – Radioactive Material and Ionizing-Radiation-Producing Machines* are managed and controlled per requirements established by NIST O 1110.00 and the NIST Radiation Safety Officer in the Gaithersburg Radiation Safety Division (GRSD) Radiation Safety Instruction (RSI) A 1-9 GRSD Document Control, RSI A 1-10 GRSD Document Development and Maintenance and the GRSD Records and File Plan Management Directive.

- 73 d. NIST O 7100.00: *Occupational Safety and Health Management System*
- 74
- 75 e. NIST O 7300.00: *Environmental Management*
- 76
- 77 f. NIST O 7400.00: *Fire and Life Safety*
- 78
- 79 g. NIST PR 7101.15: *Safety Directive Creation, Deployment, and Revision* (under
- 80 development)
- 81
- 82

## 83 6. REQUIREMENTS

### 84 a. General Document Control Requirements

85

86 (1) SMS documents shall be approved versions of NIST directives created under the “Safety”

87 subject category per NIST O 1110.00: *Directives Management System*(DMS), or internal

88 OSHE procedures.

89

90 (a) Directive types (as defined by the DMS) used are:

- 91
- 92 i. Policy;
- 93
- 94 ii. Order;
- 95
- 96 iii. Suborder;
- 97
- 98 iv. Notice;
- 99
- 100 v. Procedure; and
- 101
- 102 vi. Guidance.
- 103
- 104

105 (b) All SMS Directives are owned by the NIST Chief Safety Officer (CSO).

106

107 (c) Orders and Suborders shall be the primary document types used to establish

108 requirements, roles, and responsibilities for SMS Programs.

109

- 110 i. Regulatory compliance plans (*e.g.*, Spill Prevention Control and
- 111 Countermeasures Plans and Hazardous Waste Contingency Plans) may also be
- 112 used to establish requirements, roles, and responsibilities. These types of

113 plans are generally required to follow a format established by the associated  
114 regulation. In these cases, an SMS Suborder or Procedure may be used to  
115 either document the regulatory plan or serve as a “parent” document that  
116 references the separate regulatory plan.

117  
118 (d) Notices may be used to establish requirements, roles, and responsibilities for SMS  
119 Programs for any matter requiring prompt action.

120  
121 (e) Procedures and Guidance documents may be used to supplement SMS Orders and  
122 Suborders.

123  
124 i. Internal OSHE procedures, including associated forms and checklists may  
125 also be used to document and implement SMS processes that apply  
126 exclusively to OSHE operations.

127  
128 (f) SMS forms (including required checklists and other checklists such as OU Self-  
129 Assessment checklists that document requirements) required for or used in  
130 conjunction with<sup>3</sup> SMS Suborders and Procedures, should be included as Appendices  
131 in those documents.

132  
133 i. If not self-explanatory, forms and checklists shall include instructions on how  
134 to use them.

135  
136 ii. SMS forms required to be used in conjunction with SMS, Orders, Suborders  
137 and Procedures shall comply with requirements established in NIST PR  
138 1000.05 Forms Management.

139  
140 (2) SMS documents shall be created, approved, and managed in compliance with the  
141 requirements of:

142  
143 (a) NIST O 1110.00; and

144  
145 (b) NIST PR 7101.15: *Safety Directive Creation, Deployment, and Revision*.

146  
147 (3) All SMS documents shall be assigned an alphanumeric identifier using the numbering  
148 system in NIST O 1110.00, Appendix E.

149  
150 (a) SMS subject categories shall be designated as follows:

---

<sup>3</sup> Examples include a checklist required to be used for a periodic regulatory inspection, optional program self-assessment checklists (since they document program requirements), and program WIP checklists.

- 151                   i. 7100 Series – Occupational Safety and Health  
152  
153                   ii. 7200 Series – Ionizing Radiation Safety  
154  
155                   iii. 7300 Series – Environmental Management  
156  
157                   iv. 7400 Series – Fire and Life Safety  
158  
159                   (b) A two-digit suffix after the series number shall be used to identify specific subject  
160                   matter areas under the subject categories (*e.g.*, 7101.10).  
161  
162                   (4) Document titles for SMS documents shall be approved by the CSO or their designee.  
163  
164                   (5) SMS documents will be formatted in accordance with the document templates contained  
165                   in NIST O 1110.00.  
166  
167                   (a) In cases where no format exists or new document types are created (*e.g.*, internal  
168                   OSHE procedures), the general template requirements in NIST O 1110.00 or format  
169                   specified by the CSO will apply.  
170  
171                   (6) SMS documents shall, as appropriate, explicitly indicate the following information in the  
172                   corresponding section:  
173  
174                   (a) “References” section – shall include all relevant non-OSHE NIST documents and  
175                   external documents.  
176  
177                   (b) “Applicable NIST SMS Suborders” section – shall include all relevant references to  
178                   other SMS Suborders.  
179  
180                   (c) “Appendices” – shall include a Revision History as Appendix A, which provides a  
181                   detailed list of current changes as well as a history of previous versions.  
182  
183                   (7) SMS Suborder, Procedure and Notice documents shall, where applicable, explicitly  
184                   include the following information in the “Requirements” section:  
185  
186                   (a) Training requirements;  
187  
188                   (b) Recordkeeping requirements (for additional requirements, see Section 6.g below),  
189                   and;  
190

191 (c) Monitoring requirements, identified in the Occupational Health and Safety, Fire and  
192 Life Safety, and Environmental Management Orders.

193  
194 (8) Approved SMS documents shall have the approval date and effective date of the current  
195 version on the front page, and a footer on every page listing the version number and page  
196 number in the format “Page # of #”. Appendices pages are included in the total count.

197  
198 (9) SMS documents shall have a footer stating, "Uncontrolled Copy in Print".

199  
200 b. New Documents

201  
202 (1) SMS documents shall be created as needed to establish and comply with the requirements  
203 of the NIST SMS.

204  
205 (a) New SMS documents may be identified through any number of mechanisms  
206 including, but not limited to:

207  
208 i. SMS Management Review and other planning processes;

209  
210 ii. Internal and external audits or assessments;

211  
212 iii. Evaluations of safety-related incidents;

213  
214 iv. Relevant regulatory requirements; and

215  
216 v. Other requirements to which NIST subscribes.

217  
218 (2) The creation and approval of new SMS documents shall comply with, as applicable, the  
219 requirements established in

220  
221 (a) NIST O 1110.00; and

222  
223 (b) NIST PR 7101.15.

224  
225 (3) SMS documents shall be prepared using standard word processing software.

226  
227 c. Document Maintenance

228  
229 (1) SMS documents shall be reviewed to ensure they are still accurate and relevant:

230

- 231 (a) At least annually; or  
232  
233 (b) When any substantial relevant change occurs (e.g., change in NIST's goals, safety  
234 issues, or regulatory requirements).  
235  
236 (2) Document reviews will be carried out by the assigned Program Manager (PM).  
237  
238 (3) On an annual basis, the PM for each SMS document will be responsible for reviewing the  
239 referenced external documents to ensure they are still accurate, relevant, available and  
240 accessible, and to ensure the most recent revision is in use.  
241  
242 d. Revision of Documents  
243  
244 (1) SMS documents shall be revised in a timely manner when the associated requirements,  
245 responsibilities, or other substantive information in them changes (e.g., due to a  
246 regulatory or policy change). Revisions to SMS documents may be proposed at any time  
247 by stakeholders, the Directive Owner, or the PM.  
248  
249 (2) The revision of SMS documents shall comply with, as applicable, the requirements  
250 established in:  
251  
252 (a) NIST O 1110.00; and  
253  
254 (b) NIST PR 7101.15.  
255  
256 (3) SMS Checklists and forms included in appendices of Suborders and Procedures may be  
257 revised separately from the parent document if the revisions don't require changes to the  
258 parent document.  
259  
260 (4) The version date and number and effective date will be updated when the revision  
261 process is complete.  
262  
263 e. Communication and Distribution of Controlled Documents  
264  
265 (1) The status and availability of approved SMS documents shall be communicated to the  
266 appropriate audiences per the procedures and requirements established in NIST PR  
267 7101.15.  
268

- 269 (2) Distribution of SMS Policies and Orders shall be through the NIST Directives  
270 Management System (DMS). These documents are distributed through the DMS via  
271 links to official copies maintained within the NIST Safety website.  
272
- 273 (3) Distribution of all other approved SMS documentation shall be through the use of the  
274 NIST Safety – Document Center website and NIST Safety Website Program pages only.  
275
- 276 (a) External documents shall be maintained by the associated Program Manager in a  
277 manner that is appropriate to the use of the document (*e.g.*, some external documents  
278 may be stored on the Document Center website, and others such as instrument  
279 manuals that are used only by OSHE personnel may be maintained as an electronic or  
280 hard copy in another location.  
281
- 282 (4) Paper copies of SMS documents shall be considered uncontrolled unless one of the  
283 following conditions exists:  
284
- 285 (a) The document is printed on the day of use;  
286
- 287 (b) The document is used for training purposes; or  
288
- 289 (c) The document is used for auditing purposes.  
290
- 291 (d) The user verifies the official electronic copy has not changed, initials the hardcopy,  
292 and writes the current date next to the revision date.  
293
- 294 (5) NIST SMS documents posted in the DMS or on the NIST Safety Website will  
295 immediately supersede previous versions of the same documents.  
296
- 297 (a) Superseded documents shall be watermarked “Obsolete” and archived as electronic  
298 records in the Records Storage repository of the OSHE Documents and Record  
299 Center unless a hard copy is necessary for legal or knowledge preservation purposes.  
300
- 301 (b) To ensure the current version of a hard copy document is being used, the hard copy  
302 document should be compared to the version posted on the website.  
303
- 304 (6) The Document and Records Control (DARC) PM or designee shall:  
305
- 306 (a) Post the current version of the SMS document on the NIST Safety Website; and  
307

308 (b) Archive the obsolete document in the Records Storage repository of the OSHE  
309 Documents and Record Center.

310

311 f. Other Controlled Information

312

313 (1) Web Content

314

315 (a) The PM for each SMS program shall be responsible for ensuring web content is  
316 consistent and up to date with documented program information (e.g., Suborder  
317 content).

318

319 (b) Web content shall not establish new policy or requirements beyond those established  
320 in existing directives. (Web content may convey information about regulatory  
321 requirements or other requirements to which NIST subscribes (e.g., an ANSI  
322 Standard) that are not covered in an existing directive.).

323

324 (c) Web content may be used to communicate established policy and requirements, and  
325 supplement documented program information by providing guidance and  
326 information. It can also be used to convey other information as needed to meet the  
327 objectives of the Safety Management System (e.g., safety bulletins, best practices,  
328 and product recalls).

329

330 (d) SMS Web content shall be controlled using permissions that restrict editing and  
331 publishing of content according to procedures.

332

333 (2) Training Materials

334

335 (a) Training materials are used to communicate information and shall not establish  
336 policies or requirements beyond those established in existing directives. (Training  
337 may convey information about regulatory requirements or other requirements to  
338 which NIST subscribes (e.g., an ANSI Standard) that are not covered in an existing  
339 directive.)

340

341 (b) Content of SMS training materials shall be controlled by the PM for each SMS  
342 program.

343

344 (c) The PM shall be responsible for ensuring the content of training materials, including  
345 training materials provided by external entities, is consistent and up to date with  
346 documented program information.

347

348 g. General Requirements for Records

349

350 (1) Records shall be maintained, per the requirements of an SMS document, to demonstrate  
351 conformance to the requirements of the NIST SMS.

352

353 (2) SMS records shall be managed per the requirements of NIST O 1601.00: *Records*  
354 *Management*.

355

356 (3) Specific SMS recordkeeping requirements, including all relevant regulatory  
357 recordkeeping requirements, shall be identified in SMS documents.

358

359 (4) For each SMS record identified, the following information shall be established by the  
360 PM:

361

(a) Record Owner;

363

(b) Record Name (*e.g.*, Air Permit Compliance Program Regulatory Correspondence,  
364 Hazardous Waste Manifests, Initial Reports of Unsafe Working Conditions, Expired  
365 Confined Space Permits);

367

(c) Method by which it will be uniquely identified from other records of the same type  
368 (*e.g.*, Employee Name for Annual Audiology Exams, Date for Stormwater  
369 Inspections);

371

(d) Method by which it will be indexed (*e.g.*, Case Number, Alphabetical by Last Name);

373

(e) Security category, if applicable (either Non-Sensitive or Controlled Unclassified  
374 Information (CUI), per DOC CUI Policy and DOC CUI Guidelines);

376

(f) Format (*e.g.*, paper or electronic);

378

(g) Storage location (see Section 6.j below);

380

(h) Retention time (see Section 6.k below);

382

(i) Authorized Users (for records containing CUI); and

384

(j) The type of information contained in the record.

386

387 (5) The DARC PM shall maintain an SMS Records Master List containing the information  
388 specified in Section 6.g(4)(a)-(j) for each SMS document.

389  
390 (a) The PM for each SMS program shall provide the information specified in Section  
391 6.g(4)(a)-(j) for each program record to the DARC PM, including updates if the  
392 required information changes.

393  
394 h. Format of Records

395  
396 (1) SMS records may be in paper or electronic format, including paper records that are  
397 scanned and stored electronically. (Electronic format is preferred if possible.)

398  
399 (a) Web applications may be used to create and store records<sup>4</sup>.

400  
401 i. If a specific web application is required to create a record, it shall be identified  
402 in the SMS program document that established the recordkeeping  
403 requirement.

404  
405 (2) The following information shall be contained on/in the record, whether paper or  
406 electronic:

407  
408 (a) Record Name;

409  
410 (b) Unique identifier;

411  
412 (c) Date the record is created; and

413  
414 (d) If categorized as CUI, markings in accordance with the DOC CUI Policy and DOC  
415 CUI Guidelines.

416  
417 (3) If a specific paper or electronic form or checklist is required to be used for an SMS  
418 record, a template of the form or checklist shall be provided as an Appendix in the parent  
419 SMS document<sup>5</sup>.

420  
421 i. Creation and Filing of Records

422  
423 (1) SMS records shall be complete and legible.

---

<sup>4</sup> Examples include IRIS Reports and completed WIRS Inspection Checklists.

<sup>5</sup> This does not apply to checklists with customized content, such as WIRS checklists created by OUs, or forms contained in web applications.

424 (2) SMS records shall be filed in a timely manner, in accordance with the location and  
425 indexing information in the SMS Records Database.

426

427 j. Records Storage

428

429 (1) A storage location shall be established for each SMS record.

430

431 (2) Paper Records

432

433 (a) The storage location shall be specific, including, at a minimum, the following  
434 information:

435

436 i. Campus;

437

438 ii. Building;

439

440 iii. Room number; and

441

442 iv. Storage “unit” (*e.g.*, filing cabinet, desk drawer)

443

444 (b) The storage location shall be readily accessible to Authorized Users.

445

446 i. Physical keys used to secure CUI shall be maintained by the Record Owner  
447 and their immediate Supervisor.

448

449 (c) Paper records shall be stored in an environment that protects them from physical  
450 damage and deterioration (*e.g.*, from moisture, sunlight) as well as theft.

451

452 (d) Paper records categorized as CUI shall be restricted to Authorized Users in  
453 accordance with the DOC CUI Policy and DOC CUI Guidelines, including being  
454 stored in a locked office, locked drawer, or locked file cabinet whenever it is  
455 unattended

456

457 i. If cleaning or maintenance personnel are allowed into private offices after  
458 hours, CUI within those offices must be secured (*e.g.*, in a locked desk drawer  
459 or locked file cabinet).

460

461

462

463

- 464 (3) Electronic Records  
465  
466 (a) Electronic records shall be stored on a secure, centrally maintained NIST file server  
467 or on NIST’s cloud-based storage solutions.  
468  
469 (b) The storage location shall be specific, including, at a minimum, the following  
470 information:  
471  
472 i. Specific IT application (*e.g.*, IRIS, WIRS, ATS, CIMS);  
473  
474 ii. Path; or  
475  
476 iii. Link.  
477  
478 (c) Access to electronic records shall be controlled with password or permission settings.  
479  
480 i. Passwords to secure CUI shall be maintained by the Record Owner and their  
481 immediate Supervisor.  
482

483 k. Retention and Disposal of Records  
484

- 485 (1) A retention time, in years, shall be established for each SMS record, in accordance with  
486 the National Archives and Records Administration General Records Schedule or the  
487 NIST Comprehensive Record Schedules as applicable.  
488  
489 (a) The retention time establishes both the minimum and maximum amount of time that  
490 SMS records will be kept.  
491  
492 (2) If a retention time has been established for an SMS record by an applicable federal, state,  
493 or local regulation, it shall be the retention time used by NIST.  
494  
495 (3) SMS records should be destroyed as retention times are satisfied, unless required for  
496 business use.  
497  
498 (4) Destruction of SMS records containing CUI, including in electronic form, shall be  
499 accomplished in a manner that makes it unreadable, indecipherable, and irrecoverable.  
500  
501  
502  
503

504 1. Records Maintenance

505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543

(1) Annual Records Review

The Record Owner shall review the SMS Records Master List on an annual basis to confirm the information (*e.g.*, location, retention time) for their record(s) is still accurate.

(a) Any necessary changes to the information in the SMS Records Database shall be communicated to the relevant PM and the DARC PM.

(2) Changes or Corrections to Paper or Scanned Electronic Records

If a correction or change is required on a paper or scanned electronic SMS record, the following procedure shall be followed:

(a) Draw a single line through the incorrect or improper entry – do not erase or obscure (white-out or correction tape) the original information.

(b) Use blue or black ink to enter the correct information above the error.

(c) Record the initials of the person making the correction or change and the date next to the correction.

(d) For scanned electronic records, print the record, make changes per steps (a) through (c) above, and re-scan the corrected/changed record.

(3) Change or Corrections to other Electronic Records

If a correction or change is required on an electronic SMS record (*e.g.*, a record generated by a web application), the following shall be documented in a history log for the record:

(a) The time and date of the change;

(b) The information changed; and

(c) The individual making the change.

(4) Lost Paper Records

If a paper SMS record is determined to be lost:

(a) The most current form of the record, or if no previous record exists, the source of information used to create the original record, shall be used to reconstruct the original entries;

544 (b) The new record shall be marked “Duplicate Original – Original Lost”, signed by the  
545 individual who reconstructed the record, and dated.

546

547 (5) Lost Electronic Records

548 Lost electronic SMS records shall be restored from one of the backup servers maintained  
549 for this purpose, if possible.

550

551 (6) Damaged<sup>6</sup> Paper Records

552 If an SMS record is found to be damaged:

553

554 (a) The most current form of the record shall be used to reconstruct the original entries;

555

556 (b) The new record shall be stamped “Duplicate Original – Original Damaged”; and

557

558 (c) The damaged original shall be attached to the reconstructed record.

559

560 (7) Damaged Electronic Records

561 Damaged electronic records shall be restored from one of the backup servers maintained  
562 for this purpose, if possible.

563

564

## 565 7. DEFINITIONS

566 Definitions common to all NIST OSHE suborders can be found in Section 6 of the parent NIST  
567 Order. The definitions specific to this suborder are as follows

568

569 a. Controlled Unclassified Information (CUI) – Information the government creates or  
570 possesses, or that an entity creates or possesses for or on behalf of the government, that a  
571 law, regulation, or government-wide policy requires or permits an agency to handle with  
572 safeguarding or dissemination controls.

573

574 b. Document – A policy, process, procedure, source of information, explanation or work  
575 instruction. NIST Directives are documents; see NIST O 1110.00 for more information on  
576 types of documents.

577

578 c. Document Control – Process for approving documents for adequacy prior to issue, reviewing,  
579 updating, and re-approving documents as necessary, ensuring the revision status of  
580 documents are identified, ensuring availability of relevant versions of documents at the point  
581 of use, ensuring documents remain legible and identifiable, ensuring outdated document

---

<sup>6</sup> A record is considered damaged if the information required by 6.h.(2), or the information the record is intended to preserve is no longer complete and/or legible.

582 versions are removed from use and circulation, ensuring that only the latest, authorized  
583 document versions are in circulation, and ensuring that documents of external origin that are  
584 necessary for the SMS are properly identified and their distribution controlled.

585

586 d. Documented Program Information – Information in SMS Program documents (*e.g.*,  
587 suborders, guidance) that have been developed using the process in NIST S 7101.XX Safety  
588 Program Creation, Deployment, and Revision.

589

590 e. External Document – Documented information of external origin, necessary for the planning  
591 and implementation of the NIST SMS. Examples include national and international  
592 standards, current regulatory permits, instrumentation instruction manuals, regulations and  
593 building codes.

594

595 f. Internal OSHE Procedure – An SMS document defining a series of actions, tasks or  
596 operations or processes performed internally by OSHE to fulfill requirements of the NIST  
597 SMS.

598

599 g. Record – Objective evidence of activities performed, or results achieved related to the NIST  
600 SMS. Examples of records include but are not limited to air monitor calibrations,  
601 correspondence, noise surveys, inspection reports, incident reports, injury and illness logs,  
602 safety training records, equipment certifications, internal compliance evaluations, obsolete  
603 documents, and expired regulatory permits.

604

605 h. Record Management – Process used to ensure records are identifiable, complete, legible,  
606 readily retrievable, and stored in a manner that protects them from damage or loss.

607

608 i. SMS Document – A document developed within the framework of this document, to  
609 implement or provide guidance related to some element or requirement of the NIST SMS.

610

611

## 612 **8. ACRONYMS**

613 Acronyms common to NIST OSHE suborders can be found in Section 7 of the parent NIST  
614 Order. The acronyms specific to this suborder are as follows:

615

616 a. CSO – Chief Safety Officer

617

618 b. CUI – Controlled Unclassified Information

619

620 c. DARC – Document and Record Control

621

- 622 d. DOC – Department of Commerce
- 623
- 624 e. DMS – Directives Management System
- 625
- 626 f. NIST – National Institute of Standards and Technology
- 627
- 628 g. OSHE – Office of Safety, Health, and Environment
- 629
- 630 h. PM – Program Manager
- 631
- 632 i. SMS – Safety Management System
- 633
- 634

## 635 **9. RESPONSIBILITIES**

636 Roles and responsibilities common to NIST OSHE suborders can be found in Section 8 of the  
637 parent NIST Order. The roles and responsibilities specific to this suborder are as follows:

- 638
- 639 a. The NIST CSO is responsible for overall implementation of this Suborder.
- 640
- 641 b. The Documents and Records Control Program Manager is responsible for:
  - 642
  - 643 (1) Maintaining the NIST Document and Records Center;
  - 644
  - 645 (2) Maintaining the SMS Records Master List; and
  - 646
  - 647 (3) Maintaining the SMS External Document Inventory.
  - 648
- 649 c. Program Managers are responsible for the following, for each SMS program they are  
650 assigned:
  - 651
  - 652 (1) Developing and revising the content of program documents, and serving as the point of  
653 contact for these;
  - 654
  - 655 (2) Conducting annual program document maintenance, to include reviews of external  
656 documents;
  - 657
  - 658 (3) Ensuring web content and the contents of training materials are consistent and up to date  
659 with documented program information;
  - 660
  - 661 (4) Identifying SMS records and Record Owners for each; and

662 (5) Providing records information required for the SMS Records Database to the DARC PM,  
663 including updates as necessary.

664

665 d. Record Owners are responsible for ensuring that the SMS records they are assigned  
666 (including records stored in web applications) are created, filed, stored, retained and  
667 maintained in accordance with this Suborder and the information in the SMS Records  
668 Database.

669

670

671 **10. AUTHORITIES**

672 There are no authorities specific to this suborder alone. For authorities applicable to NIST  
673 OSHE suborders, see section 9 of the parent NIST Order.

674

675

676 **11. DIRECTIVE OWNER**

677 Chief Safety Officer

678

679

680 **12. APPENDICES**

681 A. Revision History

682

683

684  
685

**Appendix A. Revision History**

Version No.	Approval Date	Effective Date	Brief Description of Change; Rationale
0	06/14/23	06/14/23	<ul style="list-style-type: none"><li>• None – Initial document</li></ul>

686