DỰ THẢO KHUNG THAM CHIẾU XÂY DỰNG TIÊU CHUẨN

Đề nghị đổi tên tiêu chuẩn thành "BẢO MẬT DỮ LIỆU CHO HỆ THỐNG THU PHÍ ĐIỆN TỬ KHÔNG DỪNG SỬ DỤNG CÔNG NGHỆ RFID VỚI THẺ THỤ ĐỘNG"

SP 800-98 Guidelines for Securing RadioFrequency Identification (RFID) Systems.

ISO/TS 19299:2020 Electronic fee collection - Security framework.

Thông tư 12/2022/TT-BTTTT

Nội dung tiêu chuẩn	**SP 800-98:2007**	**ISO/TS 19299:2020**	TCCS 44: 2022/TCĐBVN	**TC khác**	**Phương pháp**
1 PHẠM VI ÁP DỤNG	1.2 Purpose and Scope	1 Scope			Tham khảo
2 TÀI LIỆU VIỆN DẪN		2 Normative references	2. Tài liệu viện dẫn		Tham khảo
3 THUẬT NGỮ VÀ ĐỊNH NGHĨA	Appendix B—Glossary	Terms and definitions	3. Thuật ngữ, định nghĩa và chữ viết tắt	Điều 3 TCVN 11930; TCVN 27001;	Tham khảo
4 CÁC THUẬT NGỮ VIẾT TẮT	Appendix C—Acronyms and Abbreviations	4 Abbreviated terms	3.2 Các chữ viết tắt		Tham khảo

Nội dung tiêu chuẩn	SP 800-98:2007	ISO/TS 19299:2020	TCCS 44: 2022/TCĐBVN	TC khác	Phương pháp
5 Mô hình hệ thống thu phí điện tử không dừng (ETC)			**5.1 Mô hình hệ thống ETC và các phân hệ**		
5.1 Hệ thống Front-End					
5.2 Hệ thống Back-End					
5.3 Hệ thống kết nối giữa các Back-End					
6 Khung bảo đảm an toàn thông tin cho hệ thống ETC		**6 Security requirements**			**Tham khảo**
6.1 Yêu cầu bảo đảm an toàn hệ thống ETC theo cấp độ				Thông tư số 12/2022/TT-BTTTT; TCVN 11930:2017.	
6.1.1 Yêu cầu chung					
6.1.2 Các yêu cầu cơ bản về quản lý					
6.1.3 Các yêu cầu cơ bản về kỹ thuật					

Nội dung tiêu chuẩn	**SP 800-98:2007**	**ISO/TS 19299:2020**	TCCS 44: 2022/TCĐBVN	**TC khác**	**Phương pháp**
6.1.4 Các yêu cầu khác					
6.2 Yêu cầu Hệ thống quản lý an toàn thông tin cho hệ thống ETC - Tổ chức chủ quản hệ thống thu phí điện tử phải thiết lập, triển khai, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin (ISMS) phù hợp với các yêu cầu quy định tại Điều 4 TCVN ISO/IEC 27001. - Ban quản lý cấp cao của chủ quản hệ thống thu phí điện tử cần chứng minh sự lãnh đạo và cam kết đối với hệ thống quản lý an toàn thông tin, thiết lập chính sách và phân công rõ trách nhiệm và quyền hạn trong chỉ đạo điều hành và thực thi đảm bảo ATTT tuân thủ Điều 5 của TCVN ISO/IEC 27001. - Tổ chức chủ quản hệ thống ETC phải xác định và áp dụng một quy trình đánh giá rủi ro, quy trình xử lý rủi ro, thiết lập các mục tiêu ATTT ở các chức năng và mức độ thích hợp theo quy định tại Điều 6 của TCVN ISO/IEC 27001.		6.2 Information security management system		TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013)	Tham khảo

Nội dung tiêu chuẩn	**SP 800-98:2007**	**ISO/TS 19299:2020**	TCCS 44: 2022/TCĐBVN	**TC khác**	**Phương pháp**
- Tổ chức chủ quản hệ thống ETC phải xác định và cung cấp nguồn nhân lực cần thiết cho việc thiết lập, triển khai, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin cho ETC tuân thủ theo Điều 7 của TCVN ISO/IEC 27001. - Tổ chức chủ quản hệ thống ETC phải tổ chức vận hành hệ thống ETC tuân thủ Điều 8 của TCVN ISO/IEC 27001. - Tổ chức phải cam kết liên tục cải tiến hệ thống quản lý an toàn thông tin cho phù hợp, đầy đủ và hiệu quả tuân thủ theo Điều 9 của TCVN ISO/IEC 27001.					
6.3 Yêu cầu bảo đảm an toàn thông tin cho hệ thống Front-End			4. Yêu cầu kỹ thuật của thiết bị đầu cuối (thẻ và đầu đọc)		
6.3.1 Yêu cầu chung					
6.3.2 Bảo đảm an toàn thông tin giao diện kết nối giữa thẻ RFID và đầu đọc thẻ					

Nội dung tiêu chuẩn	**SP 800-98:2007**	**ISO/TS 19299:2020**	TCCS 44: 2022/TCĐBVN	**TC khác**	**Phương pháp**
6.3.2.1 Yêu cầu kỹ thuật của thẻ RFID					
6.3.2.2 Yêu cầu kỹ thuật của thiết bị tìm đọc/ đầu đọc thẻ RFID					
6.3.3. Bảo đảm an toàn thông tin giao diện kết nối giữa đầu đọc thẻ RFID với hệ thống CNTT tại trạm					
6.4 Yêu cầu bảo đảm an toàn thông tin cho hệ thống Back-End					
6.5 Yêu cầu bảo mật tại giao diện kết nối giữa các Back-End					
6.6 Yêu cầu an toàn thông tin cho việc lưu trữ dữ liệu	**3.3.3 Network Connectivity and Data Storage** - Khi dữ liệu được lưu trữ tập trung trên máy chủ cơ sở dữ liệu, thẻ chỉ cần chứa một số nhận dạng, liên kết thẻ với thông tin được liên kết đến nó. Trong kiến trúc này, phần lớn quá trình xử lý dữ liệu xảy ra trên các hệ thống hỗ trợ mà đầu đọc được kết nối. - Mặt khác, khi dữ liệu được lưu trữ trên các thẻ, các thẻ phải có một số dạng bộ nhớ và hỗ trợ cả	6.4 Data storage		TCVN 10849: Điểm d mục 5.3.4 về Yêu cầu phân cấp bảo mật đối với CSDL lưu trữ được thực hiện	Tham khảo

Nội dung tiêu chuẩn	SP 800-98:2007	ISO/TS 19299:2020	TCCS 44: 2022/TCĐBVN	TC khác	Phương pháp
	giao dịch ghi và đọc. Bất kể dữ liệu được lưu trữ ở đâu, tính toàn vẹn của dữ liệu phải được bảo vệ. Nếu dữ liệu nhạy cảm, tính bí mật của nó cũng phải được bảo vệ. Các phương pháp để đạt được điều này bao gồm xác thực, kiểm soát truy cập, mã hóa và bảo mật vật lý. **3.4.1 Data Collection Requirements** Dữ liệu thu thập phải được theo dõi hoặc quản lý và sử dụng theo đúng mục đích như được quy định để đảm bảo rằng các điều kiện lưu trữ hoặc sử dụng phục vụ hoạt động thu phí.			theo 5 cấp.	
6.7 Yêu cầu đối với các nhà cung cấp dịch vụ thu phí		6.6 Toll service provider			Tham khảo
7 Các biện pháp bảo đảm an toàn thông tin cho hệ thống ETC		**7 Security measures — Countermeasures**			**Tham khảo**

Nội dung tiêu chuẩn	**SP 800-98:2007**	**ISO/TS 19299:2020**	TCCS 44: 2022/TCĐBVN	**TC khác**	**Phương pháp**
7.1 Các biện pháp bảo mật chung		***7.2 General security measures***			***Tham khảo***
7.2 Biện pháp bảo đảm an toàn thông tin hệ thống Front-End	***5.3.2 RF Interface Protection***		***4.1 tại TCCS 44: 2022/TCĐBVN***		
7.2.1 Bảo đảm an toàn thông tin ở giao diện kết nối giữa thẻ và đầu đọc thẻ - Đầu đọc và thẻ RFID phải tuân theo cùng tiêu chuẩn và thiết kế để có thể tương tác với nhau. Kết nối dữ liệu Ethernet hoặc RS 232 hoặc RS 485.			4. Yêu cầu kỹ thuật của thiết bị đầu cuối (thẻ và đầu đọc)	ISO 18000 6C/63 :2015; ISO 28560-2:2018;	
7.2.2 Bảo đảm an toàn thông tin cho thẻ RFID - Thẻ RFID bị động; Cơ chế bảo vệ mật khẩu; độ dài số bit mật khẩu; mã hóa AES 256; giao thức kết nối; Sử dụng ISO / IEC 18000-6C (860 đến 930 MHz, EPCglobal Class-1 Generation-2.					
7.2.3 Bảo đảm an toàn thông tin cho thiết bị tìm đọc/ đầu đọc thẻ RFID Giao thức hỗ trợ ISO/IEC 18000-63:2015.					

Nội dung tiêu chuẩn	**SP 800-98:2007**	**ISO/TS 19299:2020**	TCCS 44: 2022/TCĐBVN	**TC khác**	**Phương pháp**
EPCglobal Class-1 Generation-2 standard is essentially equivalent to the ISO/IEC 18000-6C standard.					
7.3 Các giải pháp đảm bảo an toàn thông tin cho hệ thống Back-End	***SP 800-98***	***7.5.2 Back end security measures (protection of the TSP back end interface).*** ***7.6.2 Back end security measures*** ***(protection of the TC back end interface)***	***5. Yêu cầu chung của hệ thống Back-End***	***TCVN 11930:2017***	
7.3.1 Bảo vệ dữ liệu trong hệ thống Back-End					
7.3.2 Bảo vệ hạ tầng hệ thống Back-End					

Nội dung tiêu chuẩn	**SP 800-98:2007**	**ISO/TS 19299:2020**	TCCS 44: 2022/TCĐBVN	**TC khác**	**Phương pháp**
7.3.3 Bảo đảm bằng biện pháp quản lý/ quản trị hệ thống					
7.3.4 Kiểm tra, đánh giá an toàn thông tin					
7.4 Biện pháp bảo đảm an toàn thông tin cho các kết nối trong hệ thống ETC					
7.4.1 Bảo đảm an toàn thông tin kết nối giữa hạ tầng CNTT trạm thu phí và hệ thống Back-End				TCVN 11930:2017	
7.4.2 Bảo đảm an toàn thông tin giao diện kết nối giữa hệ thống Front-End và hệ thống Back-End		7.3.5 Front End to TSP back end interface			
7.4.3 Bảo đảm an toàn thông tin ở giao diện kết nối giữa hệ thống tính phí giao dịch (TC) với nhà cung cấp dịch vụ (TSP)				TCVN 11930:2017	
Phụ lục A (Tham khảo) Hướng dẫn bảo đảm an toàn thông tin cho hệ thống ETC sử dụng RFID					

Nội dung tiêu chuẩn	SP 800-98:2007	ISO/TS 19299:2020	TCCS 44: 2022/TCĐBVN	TC khác	Phương pháp
Phụ lục B (Tham khảo) Yêu cầu cơ bản đảm bảo an toàn hệ thống thông tin đối với hệ thống thông tin cấp độ					
Phụ lục C (Tham khảo) Chính sách bảo mật					
Phụ lục D (Tham khảo) Các mối đe dọa và nguy cơ tấn công hệ thống thu phí điện tử không dừng					
Phụ lục E (Tham khảo) Đề xuất triển khai tập trung vào quyền riêng tư					
Thư mục tài liệu tham khảo		**Bibliography**			