شیوه نامه ارسال پاسخ کتبی (کاغذی)

- الزامی است متن شیوه نامه و پرسشنامه، عینا پرینت گردد
- الزامی است پاسخ در باکس بله یا خیر با علامت X مشخص گردد
- الزامی است در صورتیکه پاسخ هر سوال بله است مدارک الکترونیکی مربوطه را به شیوه زیر جمع آوری و کد کنترلی آنها را محاسبه سپس در باکس با خودکار آبی بنویسید.
- الزامی است در صورتیکه پاسخ به سوال منفی است، از نوشتن توضیحات خودداری گردد.
- الزامی است فقط و فقط یک فرد متخصص، شخصا ادله الکترونیکی را جمع آوری نماید.
- الزامی است جمع آوری کننده ذیل همه صفحات امضاء اثر انگشت و تاریخ جمع آوری را ثبت نماید.
- الزامی است نسخه اصل پاسخ به صورت مکتوب با پاسخ هایی که با خودکار آبی نوشته شده است به همراه رسانه انتقال حاوی ادله الکترونیک برای هیات در پاکت لاک و مهر شده ارسال گردد.

شیوه نامه ارسال ادله الکترونیکی:

فقط اگر پاسخ یک سوال مثبت است، لازم است ادله و مستندات الکترونیکی مربوطه ارسال گردد

- در یک هارد دیسک، پوشه ای با نام متناظر شماره ردیف سوال مربوطه ایجاد گردد.
- همه ادله الکترونیکی مربوط به پاسخ آن سوال جمع آوری و در آن پوشه کپی شوند.
- پوشه با فرمت zip فشرده شود.
- کد کنترلی هر فایل zip با الگوریتم SHA1 محاسبه گردد.
- سپس کد کنترلی در جعبه ذیل هر سوال ، با خودکار آبی نوشته شود.
- فایل های zip بروی رسانه انتقال (External HDD یا Flash memory یا DVD) کپی گردد و یک نسخه از آن نیز جهت بازدید حضوری بروی هارد دیسک اولیه باقی بماند.

بدینوسیله اقرار می نمایم که از قانون جرائم رایانه ای و آیین نامه های مربوطه اطلاع داشته و ادله الکترونیک توسط اینجانب در تاریخ مطابق آن قانون جمع آوری گردیده است و صحت و تمامیت آنرا تایید می نمایم و از کلیه مسئولیت های قانونی خود در این خصوص کاملا آگاه می باشم.

امضا و اثر انگشت شخص جمع آوری کننده

پرسشنامه فنی امنیتی وقایع سایبری

تاریخ واقعه ->	

۱- وضعیت لاگ های هر سطر را در تاریخ واقعه با نوشتن بله یا خیر در خانه های جدول اعلام فرمائید.

کد کنترلی ادله ->	

اگر لاگ های مربوط به بازه زمانی واقعه هم اکنون موجود می باشند، لطفا بله را نوشته و برای هر سطر جدول زیر اطلاعات الکترونیکی مربوطه زیر طبق شیوه نامه ارسال گردد.

الف- جدول مشخصات دارائی های به همراه name و dns name و آدرس های IP

ب- لاگ های همه تجهیزات دسته های زیر برای ۹۰ روز قبل و بعد از بازه زمانی واقعه که با اطلاعات فوق قابل احصا و جستجو باشد

ج- گزارشات SIEM تفکیک شده بر اساس دارائی شامل گزارش و نمودار time correlation و anormaly detection

Asset	اطلاعات دارائی در زمان واقعه در دسترس بوده است	لاگ گیری در زمان واقعه کاملا فعال بوده است	لاگ بر روی Asset ذخیره می شده است	لاگ در log server ذخیره می شده است	لاگ به SIEM ارسال می شده است	لاگ هم اکنون موجود است
کامپیوتر مبدا مرتبط با واقعه						
کامپیوترهای مقصد مرتبط با واقعه						
فایل ها و داده های تحت تاثیر واقعه						
سویچ های ، روترها و فایروال شبکه						
NTP Server						
Antivirus console						
DHCP Server						
DNS Server						
سامانه های نرم افزاری						
دیگر دارائی های متاثر						

- توضیح۱: اگر پاسخ به اولین ستون ، خیر است، پاسخ به بقیه ستون ها لزومی ندارد.

بدینوسیله اقرار می نمایم که از قانون جرائم رایانه ای و آیین نامه های مربوطه اطلاع داشته و ادله الکترونیک توسط اینجانب در تاریخ مطابق آن قانون جمع آوری گردیده است و صحت و تمامیت آنرا تایید می نمایم و از کلیه مسئولیت های قانونی خود در این خصوص کاملا آگاه می باشم.

مضا و اثر انگشت شخص جمع آوری کننده

۲-آیا وقوع واقعه در تاریخ یاد شده، موجب خسارات یا عواقبی گردیده است؟

خیر		بله		کد کنترلی ادله ->

اگر پاسخ مثبت است، اطلاعات زیر ارسال گردد.

الف- برای هر دسته از دارائی های ذکر شده در سطور جدول، میزان ارزش ریالی و خسارت وارده شده حاصل از نقض محرمانگی، صحت و دسترس پذیری را ذکر نمائید

ب- سند متدولوژی محاسبه ارزش ریالی دارائی

ج- سند محاسبات خسارت وارده

د- نسخه دارائی های آسب دیده

ه- مستندات جمع آوری شده مطابق شیوه نامه های استاندارد

و- مستندات رویه های فنی نحوه نگهداری، حفاظت ، توقیف و ارائه اطلاعات و استناد پذیری ادله الکترونیکی

دسته دارائی	آیا خسارت وارد شده ؟ بله/خیر	ارزش دارائی (میلیون ریال)	خسارت حاصل از نقض یکی از جنبه های زیر			
			محرمانگی (میلیون ریال)	صحت (میلیون ریال)	دسترس پذیری (میلیون ریال)	جمع (میلیون ریال)
فایلهای دیتا						
بانکهای اطلاعاتی						
فرایندها						
نرم افزار ها						
سخت افزار ها						
دیگر دارائی ها						
جمع خسارت						

بدینوسیله اقرار می نمایم که از قانون جرائم رایانه ای و آیین نامه های مربوطه اطلاع داشته و ادله الکترونیک توسط اینجانب در تاریخ مطابق آن قانون جمع آوری گردیده است و صحت و تمامیت آنرا تایید می نمایم و از کلیه مسئولیت های قانونی خود در این خصوص کاملا آگاه می باشم.

امضا و اثر انگشت شخص جمع آوری کننده

۳-آیا آن شرکت گواهینامه شخص ثالث مربوط به استاندارد ISO 27001 را دارد؟

اگر پاسخ مثبت است، گواهینامه و تاریخ و مستندات آن ارسال گردد.

خیر		بله		کد کنترلی ادله ->

۴-آیا در تاریخ واقعه، سامانه Log Server در آن شرکت وجود داشته است؟

اگر پاسخ مثبت است، مشخصات فنی سامانه به همراه لاگ های تاریخ واقعه ارسال گردد.

خیر		بله		کد کنترلی ادله ->

۵-آیا در تاریخ واقعه، سامانه SIEM در آن شرکت وجود داشته است؟

اگر پاسخ مثبت است، جدول مشخصات فنی و نیروی انسانی و شرکت پیمانکار ارسال گردد.

خیر		بله		کد کنترلی ادله ->

۶-آیا در تاریخ واقعه، شرکت دارای مرکز عملیات امنیت (SOC) بوده است؟

اگر پاسخ مثبت است، جدول مشخصات فنی و نیروی انسانی و شرکت پیمانکار ارسال گردد.

خیر		بله		کد کنترلی ادله ->

بدینوسیله اقرار می نمایم که از قانون جرائم رایانه ای و آیین نامه های مربوطه اطلاع داشته و ادله الکترونیک توسط اینجانب در تاریخ مطابق آن قانون جمع آوری گردیده است و صحت و تمامیت آنرا تایید می نمایم و از کلیه مسئولیت های قانونی خود در این خصوص کاملا آگاه می باشم.

امضا و اثر انگشت شخص جمع آوری کننده

۷-آیا صحت عملکرد کامپیوتر مبدا در بازه زمانی واقعه غیر قابل انکار بوده است؟

اگر پاسخ مثبت است، مستندات انکار ناپذیر منطبق بر آیین نامه اجرائی قانون جرایم رایانه ای ارسال گردد. مستندات باید نمودارهای و آمار ترافیک و فایل های شبکه در زمان وقوع واقعه حاوی مهر زمانی یا امضای الکترونیک باشد.

خیر		بله		کد کنترلی ادله ->	

۸-با توجه به اینکه واحد فاوا امکان اتصال از راه دور به رایانه ها را دارا می باشد، آیا اتصال پرسنل فاوا یا افراد دارای دسترسی admin سیستمی یا شبکه ای بگونه ای محدود شده است که فقط از ایستگاه ها و زیر شبکه های خاصی که دارای قابلیت ضبط اجباری (PAM SESSION RECORDING) و کامل و غیر قابل تغییر جلسات باشد استفاده نماید بگونه ای که برای حذف یا دستکاری آن سامانه، حضور همزمان چند مدیر شبکه لازم باشد؟

اگر پاسخ مثبت است، مستندات فنی و امنیتی سامانه ضبط جلسات شبکه و مجری مربوطه و افراد دارای دسترسی مدیریتی بروی آن ارسال گردد.

خیر		بله		کد کنترلی ادله ->	

بدینوسیله اقرار می نمایم که از قانون جرائم رایانه ای و آیین نامه های مربوطه اطلاع داشته و ادله الکترونیک توسط اینجانب در تاریخ مطابق آن قانون جمع آوری گردیده است و صحت و تمامیت آنرا تایید می نمایم و از کلیه مسئولیت های قانونی خود در این خصوص کاملا آگاه می باشم.

امضا و اثر انگشت شخص جمع آوری کننده

۹-آیا با یقین می توان گفت در بازه یک سال قبل از زمان واقعه تا زمان واقعه، مداوما اتصال راه دور به کامپیوتر مبدا کاملا غیر ممکن بوده و تمام پروتکل ها مانند remote desktop یا File Share یا Powershell یا WMIC یا ... همگی غیر فعال شده بودند؟

اگر پاسخ مثبت است ، رویه و مستندات hardening ایستگاه های کاری و مستندات اجرای این رویه های و کنترل آنها توسط پرسنل فاوا که منجر به تامین این شرایط گردیده است و مربوط به قبل از زمان واقعه است، ارسال گردد.

خیر		بله		کد کنترلی ادله ->

۱۰- آیا در بازه زمانی واقعه ، سرویس دهنده NTP برای تمام تجهیزات شبکه و سرورها و ایستگاه های کاری وجود داشته و اختلاف زمان همه با هم زیر یک ثانیه بوده است؟

اگر پاسخ مثبت است، مستندات فنی و امنیتی مربوطه ارسال گردد.

خیر		بله		کد کنترلی ادله ->

بدینوسیله اقرار می نمایم که از قانون جرائم رایانه ای و آیین نامه های مربوطه اطلاع داشته و ادله الکترونیک توسط اینجانب در تاریخ مطابق آن قانون جمع آوری گردیده است و صحت و تمامیت آنرا تایید می نمایم و از کلیه مسئولیت های قانونی خود در این خصوص کاملا آگاه می باشم.

امضا و اثر انگشت شخص جمع آوری کننده